UiO : Institutt for informatikk
Det matematisk-naturvitenskapelige fakultet

Risikohåndtering – Risky business?

Morten Weea ©, 31. juli 2013

Abstract

Risikoforståelse og risikohåndtering i informasjonssikkerhet er et vanskelig tema. For alle som jobber med risiko i informasjonssikkerhetsammenheng er de største utfordringene å finne ut i hvilken grad negative hendelser får konsekvenser på kritiske forretningsprosesser, og hvorvidt det er plausibelt at hendelsen inntreffer. Det er utviklet flere standarder for å beskrive optimale prosesser for risikohåndtering. Det er derimot ingen opplagt definisjon på risiko, og personlige følelser spiller ofte inn på risikoavgjørelser. Oppgaven tar for seg de nevnte problemstillingene og hvordan risikovurderinger blir utført hos tre forskjellige organisasjoner. Videre konkluderer den med at risikoforståelsen spiller en stor rolle i håndteringen av risiko, og foreslår en ny forståelse av risiko; risikoobjektet.

Forord

Det siste året har vært det mest spennende i mitt faglige liv. Jeg har fått lov til å dykke ned i et område av informasjonssikkerhetfaget som jeg har interessert meg sterkt for. Jeg har også vært heldig som har fått bo sammen med en så forståelsesfull kone, Line Weea, underveis. Hun har stilt opp med gjennomlesing og kritiske spørsmål under hele prosessen. Hun har også hørt på meg når jeg har måttet få ut mine tanker, selv om det har vært til ugunstige tider. Dette har vært til stor hjelp og motivasjon.

Videre vil jeg også takke mine fantastiske kollegaer i mnemonic. Den siste tiden har mnemonic fungert som mitt andre hjem, og alle som har vært til stede på kontoret har gledelig stilt opp til uformelle samtaler om oppgaven. Jeg vil spesielt takke Gjermund Vidhammer, Knut Håkon Tolleshaug Mørch og Tor Erling Bjørstad som har tatt seg ekstra tid til å lese grundig gjennom oppgaven min underveis, og kommet med velrettet og konstruktiv kritikk.

Jeg vil også få takke Mona Elisabeth Østvang, Hanne Moen, Tom Helge Skari og Mark Totton for gode og lange diskusjoner, faglige innspill og forslag til relevant litteratur. Å få være en del av GRC-avdelingen til mnemonic har gitt meg god faglig forståelse, takket være alle de flinke menneskene som jobber der.

Det har også vært en fornøyelse å ha en veileder som Audun Jøsang fra Universitetet i Oslo. Han har kommet med viktige tilbakemeldinger, forslag til litteratur og forslag til videre arbeid.

Sist, men ikke minst, vil jeg få takke min familie. Grete Marit, Ole Peter og Jens Weea. De har hele tiden vært der med motiverende ord og nysgjerrige spørsmål. Dette har gitt meg mye god energi, og har betydd mye for meg.

Tusen takk alle sammen, oppgaven ville ikke vært det samme uten dere!

- Morten

Innhold

Figurer

Tabeller

Del I

Innledning og metode

KAPITTEL 1

Introduksjon

Dette kapittelet inneholder en kortfattet oversikt over bakgrunnen for oppgaven, hva jeg skal diskutere i oppgaven og hva jeg har utelatt.

1.1 Introduksjon og bakgrunn

Dette er en masteroppgave skrevet ved Universitetet i Oslo, Institutt for Informatikk, retning *Informatics: Design, Use & Interaction*. Oppgavens hensikt er å inspirere til selvstendig tenkning rundt et tema jeg selv har valgt. I dette tilfellet dreier det seg om risikohåndtering innen informatikk, og hvordan risiko forstås. Til å se på dette har jeg hovedsakelig støttet meg på standardserien ISO 27000 og tilhørende litteratur.

Alle håndterer risiko og utfører risikovurderinger til enhver tid. Dagligdagse oppgaver som det å gå over veien eller å bytte jobb, er eksempler på aktiviteter som innebærer risikovurderinger. Mer eller mindre alle oppgaver man utfører inneholder en viss risiko, og uten å tenke bevisst over det behandler vi denne risikoen – ofte uten et sekunds nøling.

Når vi vurderer om det er trygt å krysse gaten, farer det mange tanker igjennom hodene våre. Selv om vi ikke bruker ord som "*trusselagent*", "*virkemidler*" og "*hendelse*", er prosessen den samme. Den åpenbare hendelsen man prøver å unngå, er at man blir truffet av en annen trafikant, og for å redusere risikoen for at denne hendelsen oppstår er det viktig å avdekke hvorvidt det finnes andre trafikanter, dvs. *trusselagenter*. Dersom det ikke finnes andre trafikanter, kan man kanskje vurdere det som trygt å krysse gaten og gå. Det kan også implementeres virkemidler, enten i form av lysregulering eller fotgjengeroverganger for å øke tryggheten og redusere faren for å bli påkjørt. Ikke helt ulikt en risikovurdering i en organisasjon, er man ikke helt trygg før sårbarhetsvinduet – i dette tilfellet; tiden man bruker på å krysse veien – er lukket. På grunn av dette er det viktig å kontinuerlig overvåke situasjonen og ta forholdsregler for å sørge for at man kommer trygt over.

En av grunnene til at jeg skriver denne oppgaven, er for å belyse problemstillingen ved å ha en standard for å vurdere noe som er så subjektivt som risiko. Standarder er gjerne noe som passer godt dersom man reiser bygg, borer etter olje eller skal følge minstekrav for arbeidsmiljø. Da er det snakk om at man skal gjøre det på spesifikke måter for å sikre at huset tåler regn og storm, at en brønn ikke kollapser når man starter boringen og at arbeidere ikke jobber under helsefarlige forhold. Når det kommer til risiko, så finnes det forøvrig helt forskjellige oppfatninger om hva som er et akseptabelt nivå. At soverom i nybygg skal tilføres minst $26\mathrm{m}^3$ frisk luft per sengeplass, er en målbar standard. At risiko skal være "*akseptabel*", er ikke målbart i samme grad. Her må man forholde seg til variabler som for eksempel forskjellige mennesketyper, samt ulike oppfatninger og organisasjoner. Et eksempel på dette er at det for noen er helt akseptabelt å hoppe fra et fly kun ikledd fallskjerm, mens andre vurderer det å ta telefonen når det ringer som i overkant skummelt.

Noen av hovedutfordringene med en risikovurdering er å enes om

definisjonen av risiko og hvordan denne måles, og å finne sårbarheter. Jeg kommer til å belyse denne problemstillingen fra forskjellige vinkler, hovedsakelig gjennom "konsulentbriller". Mye av informasjonen og flere av eksemplene i oppgaven er hentet fra erfaringer fra konsulentvirksomhet.

1.2 Formål og problemstilling

Formålet med oppgaven er å belyse problemstillingene rundt formelle risikovurderinger i større organisasjoner, samt å drøfte hvorvidt man har nytte av en felles standard. Som tidligere nevnt kan en person enten ha aversjon mot risiko, eller ha stor risikoappetitt. Her finnes det ingen fasit, og man trenger begge typene for å gjennomføre en balansert, grundig og riktig risikovurdering. Problemet kan være i hvilken grad man kan standardisere forholdet til risiko.

Det er foreslått løsninger og vinklinger fra både nasjonale og internasjonale standardiseringsorganer på hvordan man kan standardisere risiko. I skrivende stund holder også Standard Norge på å utvikle et nytt standardsett for å kunne evaluere risiko der angriperen har intensjon om å ramme deg – NS5830-serien [40, 41, 42]. Disse kan sees på som et supplement til den allerede eksisterende 27000-familien av standarder. På grunn av dette ønsker jeg å se på følgende hovedproblemstilling:

- ***"Hvordan bør risiko forstås, og hvordan bidrar standardserien ISO 27000 – med særlig vekt på ISO 27005, til en god forståelse og håndtering av risiko?"***

Som vi kan se, er dette en høyrelevant problemstilling for alle som må forholde seg til risikohåndtering på et profesjonelt nivå. For å forsøke å svare på dette spørsmålet, har jeg utformet en del underspørsmål. Svarene bidrar til å belyse det store bildet hva gjelder det å forholde seg til risiko – spesielt innenfor fagfeltet informatikk. Jeg kommer hovedsakelig til å ta fatt i ISO 27005 [31], da denne i hovedsak omhandler risikohåndtering.

1.2.1 Arbeidsspørsmål:

I et forsøk på å besvare hovedproblemstillingen har jeg utviklet en rekke spørsmål jeg ønsker å få svar på underveis i oppgaven. Hensikten med arbeidsspørsmålene mine er å begrense og definere området jeg ønsker å utforske – hovedsakelig for å få kartlagt grunnleggende begreper, generelle problemstillinger og eventuelle nytenkninger.

Jeg har definert tre hovedspørsmål som skal hjelpe meg med å besvare og begrunne hovedproblemstillingen min.

1. ***Hvordan påvirkes risikoarbeid i en organisasjon av risikoforståelsen?***

2. ***Hva er forutsetningen for et vellykket risikoarbeid i en organisasjon?***

3. ***Hvordan kan aktivitetene og resultatene i ISO 27005 formaliseres?***

For å besvare hovedspørsmålene har jeg også formulert en rekke støttespørsmål og hypoteser som skal sette fokus på det jeg mener må ligge til grunn for en god diskusjon:

1. ***Hvordan påvirkes risikoarbeid i en organisasjon av risikoforståelsen?***

    1.1 Hva er "**risiko**"?

    1.2 Er risiko universelt?

    1.3 Hvordan kan risiko forstås?

    1.4 Hvordan bør risikoscenarier defineres?

    1.5 Hvordan måles risiko?

        - Hvem definerer metrikkene?
        - Hvordan defineres metrikkene?

1.6 Hvem har nytte av en slik masteroppgave om risikovurdering?

1.7 Er risikoarbeid i seg selv en bevisstgjøring og opplæring?

2. ***Hva er forutsetningen for et vellykket risikoarbeid i en organisasjon?***

2.1 Hva er "**risiko**"?

2.2 Hva er "**informasjonssikkerhet**"?

2.3 Er risiko universelt?

2.4 Hvem foretar risikovurderinger?

2.5 Hva er formålet med en risikovurdering?

2.6 Hvorfor er det viktig med et forhåndsdefinert risikoakseptansenivå?

- Kan og bør dette nivået endres underveis?
- Hvem bør definere dette nivået – kunde eller konsulent?
  - Hvorfor?

2.7 Hvordan bør risikoscenarier defineres?

2.8 Hvordan er det å jobbe med standarder – i hovedsak ISO 27005 – i praksis?

2.9 I hvilken grad skal innleid konsulent figurere som lærer i risikoforståelse?

3. ***Hvordan kan aktivitetene og resultatene i ISO 27005 formaliseres?***

3.1 Hvordan sikres gode resultater ved hjelp av ISO 27005?

3.2 Hva er formålet med ISO 27000-familien?

3.3 Finnes det alternativer til ISO 27000-familien?

3.4 Er risiko standardiserbart?

3.5 Hvordan er det å jobbe med standarder – i hovedsak ISO 27005 – i praksis?

Som vi kan se er det noen av spørsmålene som er like under de ulike punktene. Dette er fordi jeg mener at ved å besvare spørsmålet, så vil det kunne gi grunnlag for å uttale meg om alle de berørte punktene.

1.2.2 Hypoteser og antagelser:

Videre har jeg noen oppfatninger av arbeid med risiko og risikovurderinger, og disse hypotesene ønsker jeg å få undersøkt videre. Følgende har vært utgangspunktene for arbeidet med oppgaven.

- Verdien av en risikovurdering er helt avhengig av bedriftens dedikasjon, motivasjon, modenhet og kompetanse for å ha noen reell verdi.
- Effektiv risikostyring oppnås kun ved forankring i organisasjonen.
- Et sunt forhold til risikohåndtering innebærer at man også er villig til å akseptere et visst risikonivå.
- Det er ikke mulig å bestemme fremtiden.
- Sakkyndiges tilgang på informasjon og tidligere erfaringer har en stor påvirkning på resultatet av en risikovurdering, både hva angår *hva* som blir analysert og *hvordan*.
- ISO 27005 er kun en løst sammensatt huskeliste over ting man bør tenke på, og sier intet om hvordan man gjør det.
- Risiko er ikke standardiserbart, og det er derfor heller ikke behov for standarder.
- Det er viktig med en godt definert risikoforståelse i bedriften for å oppnå riktige resultater ved analyse av risiko.
- Hovedmålet med risikohåndtering er ryggdekning i form av *due diligence*.

1.3 Avgrensninger

Det kunne vært mulig for meg å se nærmere på hva som skjer etter endt risikovurdering og hvordan resultatene har truffet i etterkant. Dette ville for øvrig blitt et for stort tema for denne oppgaven. Jeg har heller ikke sett i detalj på sikkerhetskulturbehovet i organisasjoner da dette også blir for vidt. Jeg har likevel inkludert litt om sikkerhetskulturen for å få et grunnlag for å diskutere risikovurderings- og -håndteringsdelen av informasjonssikkerheten.

Jeg har også definert følgende utenfor oppgavens scope; å se på i hvilken grad Demming-sirkelen i ISO 27001/27005 [28, 31] er optimal for risikohåndteringsarbeid, og hvordan min foreslåtte løsning, *risikoobjektet*, passer inn i en konsulents verktøykasse. Dette er begge områder jeg ønsker å se på ved en senere anledning.

1.4 Oppgavens oppbygning

I første del av oppgaven redegjør jeg for valg av tema og metode. Andre del består av gjennomgang av litteratur samt case-studiene mine. Avslutningsvis diskuterer jeg funnene mine, kommer med konkluderende anmerkninger og anbefaler videre arbeid.

KAPITTEL 2

Metode

2.1 Forskningsmetoder

I dette kapittelet vil jeg beskrive hvilke forskningsmetoder jeg har benyttet og begrunne valget av disse.

2.2 Valg og vurdering av metoder

I min oppgave har jeg valgt å benytte meg av case-studier, litteraturanalyse og intervjuer. Dette har jeg valgt å gjøre fordi de tre metodene komplementerer hverandre. Først ønsker jeg – ved hjelp av litteraturanalyse – å kartlegge fagfeltet før jeg begir meg ut på et case-studie. Målet med å studere forskjellige caser er å avdekke hvordan standardene blir benyttet, og i hvilken grad det er behov for standarder i reelle risikovurderinger. Casene vil hjelpe meg med å besvare mine tre hovedspørsmål definert i 1.2.1. Jeg har også sett hen til intervjuer for å få oppklart de bakenforliggende intensjonene til deltagerne i casene mine.

Min tilnærming til forskningen har hovedsakelig vært fenomenologisk. Jeg har ønsket å avdekke fenomener ved risikovurderingsprosesser, samt å forstå hvordan konseptene fremstår for de som benytter seg av dem. Jeg har også ønsket å høre deltagernes egne meninger og tolkninger for å få avkreftet eller bekreftet mine egne hypoteser, samt å få en bedre forståelse av behovet for ISO 27005.

Tekstene jeg har valgt å analysere inkluderer standarder, empirisk bevist litteratur fra bransjen og faglitteratur. Dette har jeg gjort for å fastslå hvilke retningslinjer det hersker enighet om, kartlegge potensielle problemer og for å få en alternativ vinkling på etablerte retningslinjer.

Da jeg, i kraft av mitt ansettelsesforhold hos mnemonic AS har fått tilgang til reelle caser hos reelle kunder, har jeg valgt å anonymisere disse. Alle resultater er grundig dokumentert hos mnemonic, som kan bekrefte casene. Da noe av informasjonen kan være konfidensiell eller kritisk for både mnemonic og/eller kunde, vil dette bli utelatt fra oppgaven av opplagte grunner.

Siden jeg hovedsakelig ønsket å skrive en oppgave som omhandler risikovurdering og -håndtering, har jeg funnet caser som allerede var gjennomført da jeg startet min oppgave. Begrunnelsen for valget av gjennomførte caser, er å få belyst helheten og de større linjene. Valget bidro også til at jeg kunne intervjue partene for å spørre hvorfor de tror det gikk som det gikk, og hva de så på som utfordringer underveis. I den forbindelse har jeg funnet tre forskjellige caser med forskjellig modenhetsgrad.

Det har vært viktig for meg å kunne relatere casene til litteraturen, og derfor har jeg også hatt lengre samtaler med konsulentene som har vært ansvarlige for risikovurderingene. Samtalene ble utført som semistrukturerte intervjuer. Under intervjuene har jeg også kommet med direkte innspill for å prøve å belyse situasjonen utenfra og med nye øyne. Hovedmålet mitt med denne fremgangsmåten har vært å opparbeide meg en forståelse for det som har blitt gjort, samt å få konsulentene til å dele sin egen refleksjon rundt de valgene som har vært foretatt i de aktuelle casene.

Del II

Tekstanalyse og Case-study

KAPITTEL 3

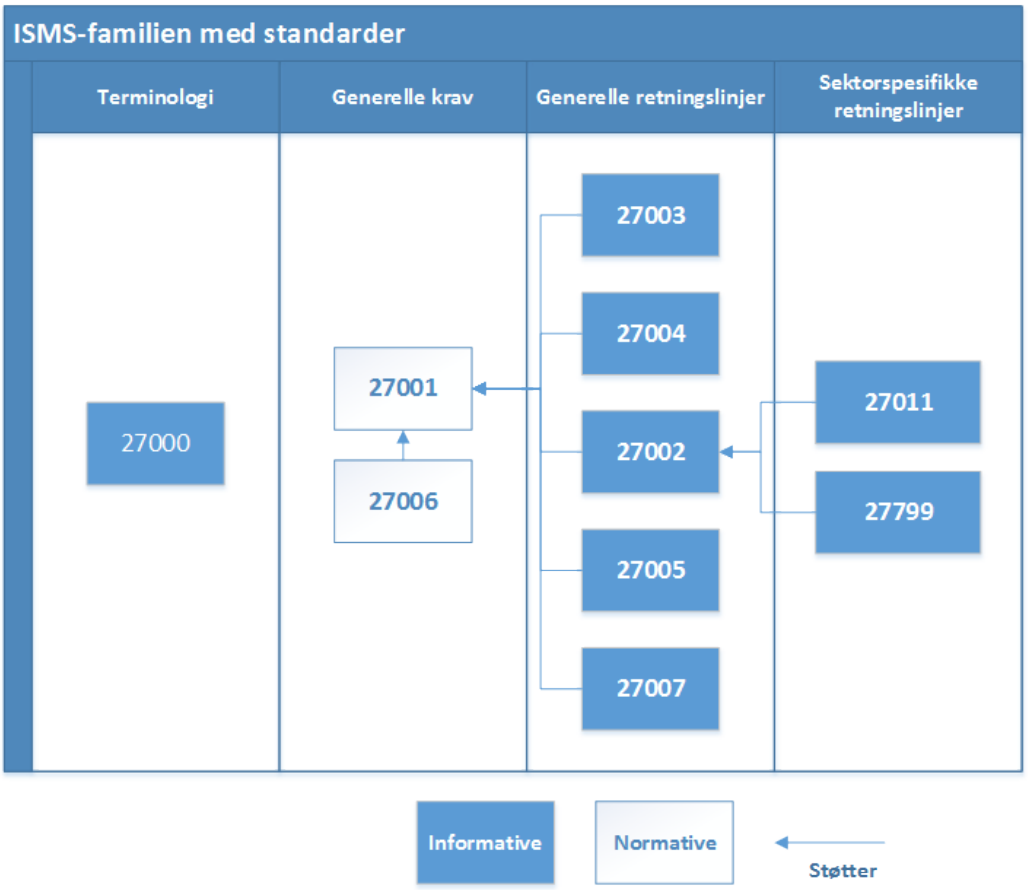
Litteratur

Jeg kommer, som nevnt, hovedsakelig til å adressere standardene for risikohåndtering og -analyse, samt bransjens behov for en felles standard – eller mangel på sådan. For å forstå sammenhengen ISO 27005 [31] er skrevet i, er det derfor også naturlig å fremheve den generelle tankegangen i ISO 27000-serien. Jeg vil også se på andre standarder og relevant faglitteratur som kan relateres til denne standardserien. Dette kapittelet kommer også til å adressere en rekke av arbeidsspørsmålene definert i 1.2.1.

3.1 Standarder

Innenfor temaet informasjonssikkerhet, er det utformet en egen serie med standarder ("ISMS family of standards") som blant annet inneholder følgende innslag – ISO 27000 [27] ISO 27001 [28], ISO 27002 [29], ISO 27004 [30] og ISO 27005 [31], hvor ISO 27005 er spesielt utformet for risikoaspektet ved informasjonsteknologi. Jeg ønsker kort å gå igjennom oppbyggingen og hensikten med disse standardene, da alle som må forholde seg til

risikovurdering og -håndtering bør ha en oversikt over dette rammeverket. Jeg har med vilje utelatt de siste standardene, selv om disse er en del av ISMS-standardfamilien. Dette fordi de havner utenfor oppgavens fokusområde. Oppbyggingen av og forholdene standardene imellom kan vi se illustrert i figur 3.1 – en tilsvarende tegning kan også finnes i ISO 27000.



Figur 3.1: ISMS-familien.

Som et supplement til disse standardene har også organisasjonen Standard Norge besluttet å utvikle en ny serie med standarder for å håndtere risiko for tilsiktede uønskede handlinger. Disse standardene er NS5830 - NS5832. Med unntak av NS5830 [40] er de to andre standardene kun ute på høring i skrivende stund, og følgelig ikke publisert. Jeg har her forholdt meg til prNS5831 [41] og prNS5832 [42] som er høringsutgaver av de kommende standardene. Det tas forbehold om endringer i forbindelse med høringsrunden.

I det følgende er det tatt utgangspunkt i det tilsiktede formålet med standarden.

I tillegg til de nevnte standardene, er det utformet en mer generell standard for håndtering av risiko; ISO 31000 [16]. Denne skal vi også se nærmere på for å forstå hvordan håndtering av risiko i andre sektorer gjøres. Det er særlig spennende å se om det er noen åpenbare likheter eller forskjeller fra risikohåndtering i informasjonssikkerhet.

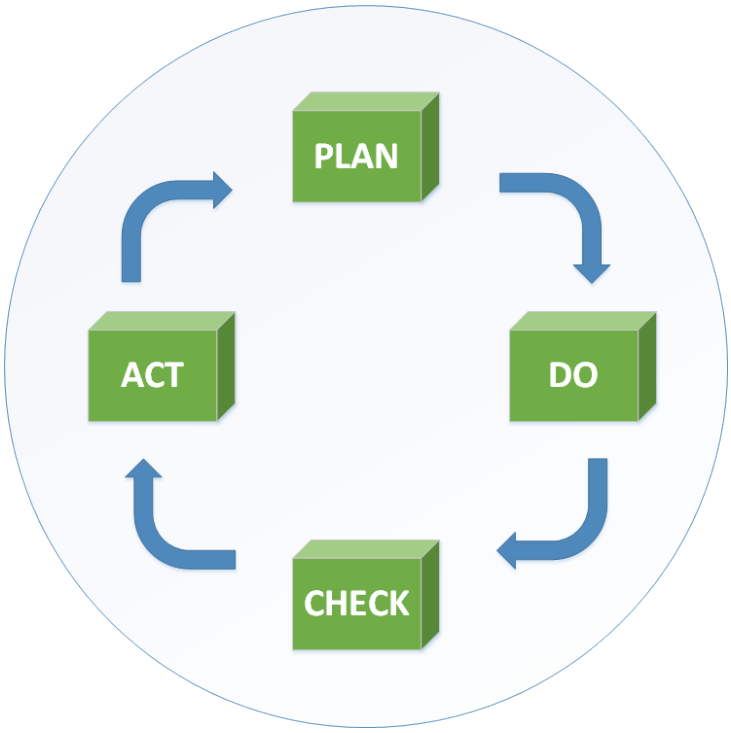
3.1.1 NS-ISO/IEC 27000:2009 Information technology – Security techniques – Information security management systems – Overview and vocabulary

Som den første i en serie på ti standarder, er det denne standarden som definerer en felles terminologi. Den tar også for seg intensjonene med resten av standardfamilien, beskriver hva ISMS er og gir en rask introduksjon til "Plan-Do-Check-Act"-modellen, eller Demming-sirkelen, utviklet av prosesskonsulenten Edward Demming for å forbedre prosesser. Dette er en viktig standard som muliggjør felles forståelse av målsetningene. Den er definert på en slik måte at den kan benyttes av alle organisasjoner som behøver eller ønsker å innføre et håndteringssystem for informasjonssikkerhet. Den tegner opp essensielle suksesskriterier for gjennomføring og innføring av ISMS samtidig som den indikerer hva som burde, men ikke trenger å være med.

I den senere tiden arbeides det med å samle terminologien i ISO Guide 73 - Risk Management – Vocabulary [17]. Dette skal binde sammen begrepsforståelsen til både ISO 27000 [27] og ISO 31000 [16], som begge er risikorelaterte standarder.

3.1.2 NS-ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements

ISO 27001 er den første av standardene som spesifikt nevner noe om hva som skal etterleves for å samsvare med Information Security Management System-standardene. Dette er en sentral standard, da de fleste som skal utføre en risikovurdering gjør det for å samsvare med ISMS. Her blir også "Plan-Do-Check-Act"-modellen omtalt og forklart, se figur 3.2.



Figur 3.2: Plan-Do-Check-Act-modellen.

Kort fortalt vil "PDCA"-modellen sørge for at det blir utviklet et ISMS i første steg. Deretter sørger den for at man skal implementere nevnte ISMS før man vurderer den og tar eventuelle korrigerende skritt. Dette er en evig syklus som sørger for at man til enhver tid har et fungerende og optimalisert ISMS.

Under kapittel 3 får man en rask innføring i de forskjellige definisjonene som standarden benytter seg av, og hvilke andre definisjoner og terminologier den baserer seg på. Kort oppsummert er dette begreper som definerer forståelsen av standardens nedslagsfelt.

Kapittel 4 er kapittelet som standardiserer hvordan et Information Security Management System skal se ut og hva det skal inneholde for å samsvare med standarden. Kapittel 4 starter med en beskrivelse av hva man skal gjøre for å etablere ISMS, hva man skal definere av mandat og avgrensninger, samt hva som er viktig for bedriften å beskytte. Etter at man har fått en oversikt over hva som er viktig for hvem i bedriften, er det neste steget å vurdere hvorvidt noen av disse verdiene er utsatt for trusler eller sårbarheter. Dersom trussel- eller sårbarhetsnivået er akseptabelt, er det ikke behov for å gjøre noe ytterligere med dette. Dersom nivået ikke er akseptabelt, må det implementeres virkemidler for å redusere trusselen til et akseptabelt nivå. Når planene for risikoreduksjon og -akseptanse er lagt, skal man implementere det man har definert, samt starte med en kompetanseutviklingsplan. Mens dette rulles ut ser man effekten av ISMS-virkemidlene og starter vurderingen av disse. For å vurdere effekten av virkemidler er det viktig å kunne måle status før og etter implementasjonen. Dette blir grundig beskrevet i ISO 27004 [30]. Dersom noe blir gjennomgått og man finner at virkemidlene ikke fungerer optimalt, skal man i følge standarden endre dem. Da er man rundt PDCA-hjulet og kan starte en ny iterasjon hvor man leter etter nye situasjoner der ISMS ikke fungerer optimalt.

Det er strenge krav til dokumentasjon av ISMS. Blant annet skal dokumentasjonen inneholde alle beslutninger tatt av ledelsen. Alt som blir bestemt, skal kunne spores tilbake til når og hvor det ble besluttet. Det er også viktig å kunne begrunne valg av virkemidler med en vurdering av risiko, gjerne i form av en risikoestimering og/eller -vurdering. En estimering er å betrakte som mer omtrentlig og uformell enn en vurdering. Videre stilles det strenge krav til kontroll og bevaring av dokumenter. Alt skal dokumenteres, og

alt skal være transparent og sporbart. Det er viktig å kunne bevise alle stegene underveis i prosessen med ISMS, samt å dokumentere konformitet med standarden hva angår besøkslogger, revisjonsresultater og endringslogger.

Det neste kapittelet – kapittel 5 – definerer ledelsens ansvar. Utover å indikere at ledelsen har et ansvar, definerer kapittelet at ledelsen skal ha et eierskap til innføringen og utviklingen av ISMS. Ledelsen har også ansvar for å tildele både midler og ansatte til arbeidet med ISMS. Hva gjelder tildeling av de menneskelige ressursene, er fokusområdene **trening**, **bevissthet** og **kompetanse**.

Kapitlene 6, 7 og 8 beskriver "Check"- og "Act"-trinnene i PDCA. Her blir prosessene med internrevisjon og forbedring av eksisterende ISMS gjennomgått. Det blir forklart hva som er målet med en internrevisjon – nemlig å avdekke uregelmessigheter og avvik fra vedtatte retningslinjer. Videre blir ledelsen minnet på at dette er noe de har eierskap til, og at de skal reagere umiddelbart for å korrigere nevnte avvik og uregelmessigheter. Det er også ledelsens ansvar å få tilbakemeldinger underveis fra de rette interessentene. Tilbakemeldingene er nødvendig for å videreutvikle ISMS, slik at den samsvarer med den retningen bedriften er på vei. Poenget med Information Security Management Systems er å være preventiv – samt at potensiell skade reduseres til et minimum.

I tillegg til de overnevnte kapitlene er det utviklet tre vedlegg. Det første er en huskeliste man kan bruke for å utvikle sin egen Statement of Applicability (SOA). Det andre vedlegget er en sammenligning mellom OECD-prinsippene [15] og "Plan-Do-Check-Act"-modellen. Det tredje og siste vedlegget viser korrelasjon mellom ISO 27001, ISO 9001:2000 (kvalitetshåndtering) [18] og ISO 14001:2004 (miljøhåndtering) [19].

3.1.3 NS-ISO/IEC 27002:2005 Information technology – Security techniques – Information security management systems – Code of practice for information security management

ISO 27002 er en liste over vanlige virkemidler. Etter å ha spesifisert hvilke definisjoner som skal benyttes i standarden, beskriver den hva som skal være formålet med en vurdering av risiko og hva bedriften bør tenke på før den implementerer virkemidler for å redusere risiko. Deretter lister den opp forskjellige scenarier, hvordan man kan kontrollere risikoen, et forslag til implementering og annen nyttig informasjon hva gjelder den omtalte risiko. Standarden kan brukes som en smørbrødliste for generelle vurderinger av ISMS i en bedrift. Det bør ikke implementeres virkemidler ukritisk, da det vil være både uhensiktsmessig dyrt og strengt å gjennomføre. Det bør gjennomføres en risikovurdering for å avdekke organisasjonens behov. Hvordan dette gjøres beskrives i ISO 27005 [31].

3.1.4 NS-ISO/IEC 27004:2009 - Information Technology – Security techniques – Information security management – Measurement

ISO 27004 er standarden som definerer hvordan man skal måle nytten og effekten av sikkerhetstiltak. I likhet med de andre standardene defineres først scope og referanser. Standarden bygger på ISO 27000 [27] og ISO 27001 [28]. Videre defineres det en del ord og uttrykk som ikke er dekket tidligere, og som skal brukes i 27004. Standarden foreslår hvordan man kan måle implementasjonen av tiltakene i ISO 27002 [29], og vil også definere ledelsens ansvarsområder. Resten av standarden forklarer litt om hvordan man skal samle inn data, og hvordan dataene skal brukes. Vedleggene eksemplifiserer hvordan det kan gjøres på en formell måte.

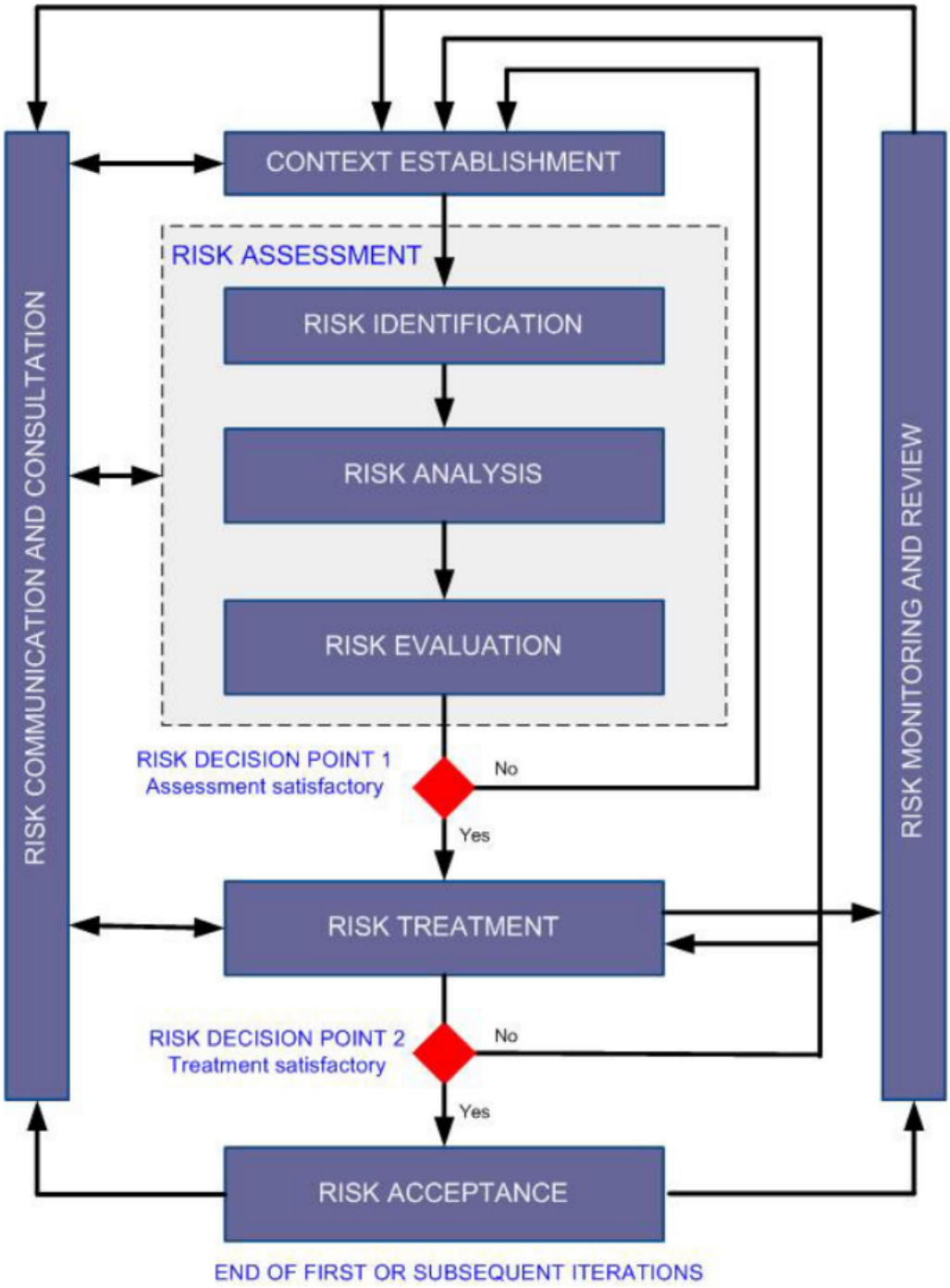
3.1.5 NS-ISO/IEC 27005:2011 Information technology – Security techniques – Information security risk management

Denne standarden omhandler risikostyring i informasjonsteknologi. Der samtlige av de andre standardene jeg har belyst til nå legger til rette for at man skal kunne utvikle en policy, er det 27005 som hjelper til med å definere risikomomentene, og hva som følgelig burde omtales i en policy. Formålet med denne standarden er å definere basiskriteriene for risikovurderinger og arbeid med identifisering av risiko. Standarden forteller *hva* man skal gjøre, og ikke så mye om *hvordan*.

Standarden definerer noen nye ord og uttrykk som ikke tidligere er nevnt i 27000-serien, eventuelt redefinerer ord slik at de bedre passer til risikovurderingen. Den beskriver videre hvorfor det er viktig med en systematisk tilnærming til risiko og hva man bør håpe å oppnå ved hjelp av en risikovurdering. Først og fremst inneholder denne strategien følgende prosesser (se 3.1 for samsvar med Demming-sirkelen):

- Etablering av kontekst
- Vurdering av risiko
- Behandling av risiko
- Akseptanse av risiko
- Kommunisering av risiko
- Gjennomgang og overvåkning av risiko

Videre illustreres det hvor i PDCA-modellen de forskjellige aspektene ved risikohåndtering kommer inn, se figur 3.3, før man blir presentert en sjekkliste med punkter man bør ta stilling til før man starter risikovurderingen – herunder



Figur 3.3: Risk management-prosessen i informasjonssikkerhet

blant annet hvorfor man gjør vurderingen, hvem som eier ansvaret og hva man kan akseptere av risiko.

I hvilken grad man kan si at Demming-sirkelen er en god rettesnor hva

Tabell 3.1: Korrespondanse mellom ISMS og risikohåndteringsprosessen

ISMS-prosess	**Risikohåndteringsprosess i informasjonssikkerhet**
Plan	Etabler kontekst Vurder risiko Utvikle plan for å behandle risiko Aksepter risiko
Do	Implementer risikobehandlingsplan
Check	Kontinuerlig overvåkning og gjennomgang av risiko
Act	Vedlikehold og forbedre risikohåndteringsprosessen

angår risikoarbeid, kan man diskutere. Den var uten tvil effektiv da den ble foreslått for Toyota. Problemet er at man sjelden kun befinner seg i én fase i et kontinuerlig risikohåndteringsarbeid; man er i alle fasene samtidig. Dette vil gjøre det vanskelig å skille mellom når man er i hvilken fase, og hva som er oppgavene i denne fasen. Dette illustreres godt i tabell 3.1. Her ser vi at *Check*-fasen inneholder den kontinuerlige driftingen, og *Plan*-fasen er fasen for å akseptere risiko. Det er ikke en intuitiv forståelse av hvordan risiko kan håndteres, og bør kanskje revurderes.

I tilknytningen til denne standarden er det også utviklet vedlegg – hele syv stykker. Vedleggene har ikke den samme tyngden som en standard har, og fungerer som foreslåtte supplement heller enn fasit. Dette er et viktig skille der man som organisasjon skal jobbe for å bli godkjent etter standarder. I min oppgave ønsker jeg å se på vedleggene som en del av standarden.

Det første av vedleggene går ganske nøye inn på hva som skal være omfanget og avgrensninger for risikohåndteringsprosessen. Først og fremst er det viktig å kjenne organisasjonen, og det fremheves et behov for å forstå **eksakt** hvordan organisasjonen er bygd opp – i den grad dette lar seg gjøre. Dette gjøres best ved å få innblikk i organisasjonens daglige virke,

og på den måten få avdekket avvik fra organisasjonskartene og opprinnelig tenkt struktur. Det er særlig tre nivåer som bør kartlegges; beslutningsnivået, ledelsesnivået og driftsnivået. Dernest påpekes det at det bør identifiseres og utarbeides lister med begrensninger for organisasjonen. Dette fordi det kan være begrensninger som ikke tidligere er identifisert, eller nye begrensninger i form av lover og forskrifter som er utviklet og har trådt i kraft siden forrige revisjon/iterasjon. De viktigste begrensningene å identifisere er uansett de man kan gjøre noe med, herunder de interne begrensningene, som budsjett og personell. I følge vedlegget er det viktig at organisasjonen setter seg langsiktige mål og utarbeider en liste over begrensninger som vil gjøre det vanskelig for organisasjonen å nå de nevnte målene.

Vedlegget har også utviklet en generell liste over begrensninger og områder man bør ta stilling til:

- Politiske begrensninger, eks. lover og regler
- Strategiske begrensninger, eks. endringer i organisasjonen som tvinger frem behov
- Territorielle begrensninger, eks. struktur som introduserer begrensninger
- Økonomiske begrensninger, eks. finanskrisen
- Strukturelle begrensninger, eks. inndeling av organisasjonen
- Funksjonelle begrensninger, eks. bemanning 24/7
- Personellbegrensninger, eks. tilganger og klareringer til gradert materiale
- Tidsbegrensninger, eks. frister på prosjekter som går på tvers av avdelinger
- Metodebegrensninger, eks. mangel på know-how eller erfaring

- Kulturelle begrensninger, eks. holdninger, rutiner, workarounds som undergraver policy

- Budsjettbegrensninger, eks. mangel på handlingskraft grunnet dårlig likviditet

Noen av de nevnte begrensningene kan også påvirke omfanget av risikohåndteringen og følgelig også endre noen av de andre nevnte begrensningene. Mangel på kunnskap, personell eller penger kan være eksempler på dette.

Videre – i vedlegg B – er det utviklet retningslinjer for å identifisere og evaluere verdier, samt hva man bør tenke på ved en konsekvensutredning. Dette deles inn i to typer verdier, primærverdier (forretningsaktiviteter og -prosesser) og støtteverdier (hardware, software, personell, nettverk, struktur og kontorer).

Når det kommer til identifisering av primærverdiene, er dette en prosess som hjelper til med å begrense og definere omfanget av risikohåndteringsprosessen. Det bør derfor også nedsettes grupper med blandet bakgrunn, slik at man lettere identifiserer kjerneprosesser i bedriften – herunder hva er det ingen klarer seg uten? Oftest inkluderes ledere, systemspesialister og brukere i dette utvalget. I dette punktet blir det også nevnt spesifikt hva som kjennetegner primærverdi-prosessene og -informasjon. Fellestrekk for primærverdiprosesser er at de ikke klarer seg uten dem, de har konfidensiell informasjon, og at organisasjonens virke blir drastisk redusert dersom primærverdiene ikke er tilstede/i drift.

Den andre delen av dette vedlegget hjelper til med å vurdere verdiene og aktiva. Her blir det informert om at man kan bruke både kvantitative og kvalitative skalaer for å vurdere sine aktiva. Noen aktiva kan måles i kroner og øre, mens andre ikke kan det, og følgelig burde man derfor benytte seg av den skalaen som fremstår som mest fornuftig. Både den kvalitative og kvantitative målestokken kan også brukes på samme aktiva/verdi – og en skala for vurderingen bør være avklart gjennom hele virksomheten. Uansett

bør det også skrives ned et entydig kriterium for å vurdere aktiva, slik at det blir mulig å sammenligne to forskjellige aktiva opp mot hverandre. Det vil være tilnærmet umulig å verdivurdere noe som er uvurderlig, f.eks. organisasjonens omdømme. Her må man sette en abstrakt verdi, men man kan for eksempel ta høyde for hva det vil koste å gjenopprette omdømmet, hvor mye man går glipp av når kundene forsvinner, et cetera.

Et aktiva kan gjerne få tilskrevet flere verdivurderinger, og den totale verdien på disse aktiva er gjerne den som avgjør hvor viktige de er for bedriften. Den endelige vurderingen avgjør da hvor mye penger som skal brukes for å beskytte det omtalte aktiva. Det er uansett viktig at alle aktiva til slutt blir vurdert over felles list, såkalt "*common base*". Dette gjør det mulig å ta de vanskelige valgene mellom hva som er mest kritisk å beskytte og hva som kan erstattes. Videre i vedlegget følger det en liste over mulige kriterier, som for eksempel; tap av omdømme, stans i produksjonen, brudd på lover.

Når man skal vurdere verdiene til et aktiva, er det fort gjort å glemme alt dette aktiva er avhengig av, og alle aktiva som er avhengig av det aktiva man skal vurdere. Det kan derfor være lurt å lage en oversikt der de mest kritiske aktiva (som flest er avhengig av) blir identifisert. Dette burde også være en faktor i verdivurderingen av alle aktiva. Man bør også ta stilling til om verdien til aktiva blir ivaretatt i alle ledd, slik at man kan identifisere prosesser som bør omarbeides.

Utfallet av verdivurderingen skal være en liste over aktiva og deres relative verdi – hvor mye de koster å erstatte, hvor mye nedetid de er skyld i dersom de forsvinner, om de lekker informasjon, et cetera.

I følge vedlegget er det også ønskelig å utføre en konsekvensutredning for å kartlegge hva som vil skje dersom man blir utsatt for en eller flere sikkerhetshendelser. En innvirkning kan ha enten en umiddelbar konsekvens (driftskonsekvens) eller fremtidig konsekvens (bedriftskonsekvens). Driftskonsekvensene deles ofte inn i direkte eller indirekte, hvor direkte konsekvenser omhandler kostnader for å reparere eller erstatte et aktiva eller tap av informasjon. In-

direkte konsekvenser omhandler at man går glipp av investeringsmuligheter fordi man må bruke penger som en direkte konsekvens, eller inntjening man går glipp av dersom produksjonen stopper som en følge av hendelsen. Det finnes også driftskonsekvenser som kan føre til bedriftskonsekvenser.

Naturlig nok vil den første konsekvensutredningen være ganske nært verdivurderingen av aktiva, da ingen virkemidler er innført for å redusere konsekvensene. Dette fordi man i denne fasen ser bort ifra implementerte virkemidler – dette er en Business Impact-analyse (BIA). Jeg velger å bruke det norske ordet *konsekvensanalyse* videre i oppgaven.

De to neste vedleggene til denne standarden er lister over typiske trusler og sårbarheter, samt metoder for å vurdere sårbarheter.

Vedlegg E beskriver metoder for å utføre risikovurderinger. Det starter med en fremgangsmåte for å utføre en høynivå-risikovurdering, der man gjerne kan se på sårbarheter, trusler, aktiva og konsekvenser. Dette er typisk noe man gjør når det har gått en stund, slik at man har datamateriale å jobbe med. Dersom man ikke har datamaterialet, eller det har gått for kort tid siden man utviklet retningslinjene, kan man starte med en konsekvensutredning. Man kan gjerne utføre denne risikovurderingen innenfor spesifikke domener, og det er vanlig å evaluere en liste med trusselscenarier.

En høynivåvurdering tar gjerne for seg vanlige og generelle scenarier, og har også forslag til vide, generelle virkemidler som kan redusere risikoen for å bli utsatt for nevnte trusler og scenarier. Den vil for eksempel sjelden adressere de tekniske aspektene av sikkerhet og derfor vil høynivåvurderingen kun foreslå virkemidler som backup og antivirus – ikke hvordan backup skal utføres eller hvilken antivirus som skal benyttes.

Noen av fordelene med en slik analyse vil være at den generelle tilnærmingen til risikovurderinger vil øke akseptnivået, bevisstheten og forståelsen for et kontinuerlig vurderingsprogram innad i organisasjonen. Det vil også være mulig å skissere en strategi for utviklingen av organisasjonens retningslinjer. Ressurser og penger kan bli tilført der man avdekker behov for dette. Selvføl-

gelig er en av farene når man utfører denne gjennomgangen på et generelt nivå, at noen prosesser eller systemer ikke blir oppdaget, som igjen fører til at man må foreta enda en analyse, denne gangen mer spesifikk.

Høynivåvurderingen vil vurdere forretningsverdien til informasjonsaktiva, og vurdere hvorvidt det er risiko tilknyttet aktiva fra et forretningsøyemed. Allerede ved første bestemmelsespunkt vil dette vedlegget kunne avhjelpe med å ta de rette valgene for hvorvidt man kan behandle risikoene, eller må gå videre i prosessen. Noen av kriteriene man kan basere vurderingene på, er for eksempel hvorvidt man kan nå forretningsmålene med eller uten nevnte aktiva, i hvilken grad bedriften er avhengig av nevnte aktiva for sin daglige drift, kostnadene ved å være uten nevnte aktiva – indirekte og direkte – samt hvilke aktiva organisasjonen faktisk tillegger verdi.

Når alt dette er vurdert og avdekket, kan organisasjonen identifisere hvor de skal bruke sin neste iterasjon. Dersom et aktiva er kritisk og står i umiddelbar fare for å bli angrepet, kan organisasjonen gå igang med en mer spesifikk risikovurdering av dette aktiva. Dersom første runde med vurderinger ikke er tilstrekkelig for å redusere risikoen til et akseptabelt nivå, bør det utføres ytterligere iterasjoner.

Videre beskrives det en metode for å utføre en detaljert risikovurdering for informasjonssikkerheten. I motsetning til den mer generelle høynivåanalysen beskrevet tidligere, er det i denne fasen på tide med et skikkelig nøye og gjennomgående dypdykk i prosessene og systemene. Her skal det identifiseres hvilke komponenter som innehar hvilke sårbarheter, hvor mye de forskjellige systemene er verdt, og hvilke komponenter man ikke kan klare seg uten. På denne måten er det lettere å identifisere de spesifikke truslene, og man kan utvikle og påføre behandling der den trengs. Da denne prosessen gjerne er tidkrevende, har en høy kostnad og krever høy kompetanse, bør den helst utføres på aktiva, prosesser og systemer som er utsatt for høy risiko i den innledende risikovurderingen beskrevet tidligere.

Vedlegget påpeker at konsekvensene gjerne bør klassifiseres med kvalita-

tive (høy - medium - lav - etc) og/eller kvantitative (kostnader) mål. Dette bør bedriften/organisasjonen definere i forkant, herunder hva som kan beskrives som for eksempel høy eller lav. For å kunne vurdere aktiva, bør det defineres et tidsvindu hvor nevnte aktiva har behov for beskyttelse. Det nevnes også at trusselsannsynligheten bør vurderes ut ifra følgende punkter:

- Attraktiviteten eller innvirkningen til aktiva
- I hvilken grad et aktivas sårbarhet kan konverteres til gevinst for angriper
- Angrepskompetansen og motivasjonen til trusselagenten
- Mottagelighet for sårbarheten, enten tekniske eller ikke-tekniske sårbarheter

Det er uansett kritisk at organisasjonen benytter seg av en klassifiseringsmetode som organisasjonen er komfortabel med, og som kan reprodusere tilnærmet like resultater ved en ny gjennomgang. Dette kan bli vanskelig når man skal bruke både subjektive og empiriske data.

Det første av de tre eksemplene som blir gjennomgått i vedlegget, er en matrise med forhåndsdefinerte verdier, se tabell 3.2. Her skal alle aktiva klassifiseres og settes verdi på, for eksempel på en skala fra 0 til 4. Dette kan i mange tilfeller være en fullstendig arbitrær skala, men det viktigste er at organisasjonen er konsekvent i sin inndeling, og at de kan forstå hvordan og hvorfor de har kommet frem til den klassifiseringen de ender opp med. Verdiene på aktiva utledes gjerne fra intervjuer med organisasjonens ledere og dataeiere. Aktiva bør også evalueres etter retningslinjer som tar hensyn til:

- Personlig sikkerhet
- Personlig informasjon
- Lover og forskrifter
- Rettshåndhevelse

- Kommersielle og økonomiske interesser
- Monetære tap og forstyrrelse av drift
- Ro og orden
- Forretningsretningslinjer
- Tap av omdømme
- Kundekontrakter og -avtaler

Når så alt har blitt klassifisert, er det på sin plass å se på **trusselnivået** (sannsynligheten for at en uønsket hendelse blir forsøkt gjennomført) og **sårbarhetsnivået** (sannsynligheten for at en sårbarhet kan bli utnyttet). Dette gjøres, i følge vedlegget, best ved hjelp av spørreundersøkelser. Hvert spørsmål har et svar som gir en score, og til slutt summeres alle poengene, og man ser hvilket sjikte nevnte aktiva har havnet i. Kombinerer man scoren for verdi (tidligere foreslått 0 - 4) på Y-aksen med verdiene for trusselnivå (høy - medium - lav) og sårbarhetsnivået (høy - medium - lav) på X-aksen, kan man få et skjema som i tabell 3.2, som gir en endelig verdi mellom 0 og 8, der 0 er lavest behov for beskyttelse, og 8 er det høyeste nivået.

	Likelihood of occurrence – Threat	Low			Medium			High		
	Ease of Exploitation	L	M	H	L	M	H	L	M	H
Asset Value	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Tabell 3.2: Tabell fra appendiks E i 27005.

Ved gjennomgang av listen over verdier og aktiva, og når man kommer til et aktiva eller verdi som mangler score på trusselnivå eller sårbarhetsnivå,

så betyr det at det for øyeblikket ikke finnes risiko for at dette aktiva skal bli utnyttet. Dette kan selvfølgelig forandre seg når som helst.

Man kan også benytte seg av en "forenklet" matrise (se tabell 3.3) der man måler sannsynlighet for en hendelse på den ene aksen mot effekt for forretningen på den andre aksen. Også her kan man bestemme den endelige risikoen for et aktiva ved hjelp av kvantitative eller kvalitative mål, se tabell 3.3.

	Likelihood of incident scenario	Very Low (Very Unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
Business Impact	Very Low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very High	4	5	6	7	8

Tabell 3.3: En forenklet utgave av forrige matrise.

Det neste eksemplet som blir foreslått i dette vedlegget, er å rangere truslene etter risiko. Her skal man også sette tall på konsekvens og sannsynlighet, for å multiplisere disse tallene for en endelig verdi. Hvis man for eksempel setter sannsynlighet til 2 og konsekvensen til 4, vil vi få en risiko der $4 \times 2 = 8$. Hvis man har mange risikoer og få nivåer, vil selvfølgelig en del av risikoene få samme score, og da kan man måle etter kroner og øre, for å skille 2 scenarier med samme score fra hverandre. Her bør man unngå å bruke tallet 0 i skalaen, av åpenbare grunner.

Eksempel 3 foreslår å måle verdien for sannsynligheten sammen med de mulige konsekvensene av risikoen, og ved å kombinere disse to, vil man kunne få en sannsynlighetsverdi for hendelsescenariet (se tabell 3.4). Summerer man deretter sammen alle scenariene, vil man kunne få en score for systemet, prosessen eller aktiva. Kombinerer man dette med verdien til aktiva, skal man kunne lese av en matrise (se tabell 3.5) hvor stor risiko nevnte aktiva har, lest ut ifra verdi på en akse og sannsynlighetsverdi på den andre aksen.

Likelihood of Threat	Low			Medium			High		
Levels of Vulnerability	L	M	H	L	M	H	L	M	H
Likelihood Value of an incident scenario	0	1	2	1	2	3	2	3	4

Tabell 3.4: Matrise for å regne ut sannsynlighetsverdi.

Asset Value	0	1	2	3	4
Likelihood Value					
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

Tabell 3.5: Matrise med systemets totalverdi.

For å illustrere matrisene over kan du for eksempel ha system A og system B, begge med to scenarier; (Aa, Ab) og (Ba, Bb). Videre har scenariene verdier som illustrert i tabell 3.6;

Tabell 3.6: Verdier for scenarier

Scenarier:	Aa	Ab	Ba	Bb
Sannsynlighet for trussel:	Low	High	Low	Medium
Sårbarhetsnivåer	High	Low	Low	High
Sannsynlighetsnivå	2	2	0	3

Som vi kan se av tabell 3.6, har scenario Aa samme sannsynlighetsverdi som Ab, selv om Ab i utgangspunktet har en høyere sannsynlighet for å bli utnyttet. Vi kan også observere at Bb er det scenariet med høyest sannsynlighet for å bli utnyttet, selv om det kun er medium sannsynlighet for

at det skal bli utsatt for en trussel. Hvis vi attpåtil slår sammen scenariene til misbrukssansynlighet for systemene, ser vi at $A = Aa + Ab = 4$, og $B = Ba + Bb = 3$. Altså er A i utgangspunktet mer utsatt for trusler og sårbarheter enn scenariet B er. Dersom vi attpåtil legger til aktivaverdi til systemene, kan dette snu seg. Sett at A er et ukritisk system som lett kan erstattes og at det allerede benyttes substitutter idag, mens B er et kritisk system som **må** være oppe 24/7. Da er det lett å sette *asset value* på A til 0, mens B kan vurderes som en 4, ref tabell 3.5. Da vil det plutselig se helt annerledes ut, og totalscoren til B vil overskride verdien til A da verdiene blir henholdsvis 7 og 4 i følge tabell 3.5.

Standardens nest siste vedlegg inneholder en liste over begrensninger for å innføre virkemidler. Her blir det nevnt eksempelvis tidsbegrensninger, budsjettbegrensninger og kulturbegrensninger. Felles for alle begrensningene er at de gjerne er individuelle for hver organisasjon, og egentlig ganske åpenbare. Før man skal innføre et virkemiddel er det veldig viktig å se på hvor klar organisasjonen er for nettopp dette virkemiddelet. Dersom det ikke finnes penger eller tid til å innføre et virkemiddel i vinduet man anser aktiva som sårbar, er det følgelig heller ikke noe poeng i å innføre nevnte virkemiddel. Man må også ta stilling til hvorvidt det er akseptabelt å innføre et virkemiddel som for eksempel scanning av epost. I mange land blir dette uglesett av de ansatte, og vil føre til motstand og workarounds.

Vedlegg G beskriver forskjeller fra 27005:2008 til 27005:2011. Her er det minimale forandringer. Hovedsakelig er det endringer i terminologien, og en del ord har blitt tilført for å skape klarhet, eventuelt for å reformulere noen av de allerede eksisterende definisjonene.

3.1.6 AS/NZS ISO 31000:2009 Risk management – Principles and guidelines

I likhet med 27001 [28], er 31000 mer overordnet. Det er en relativt kort standard, som tar for seg terminologi og mandat. Samtidig foreslår den prosesser og et rammeverk for å behandle risiko. I motsetning til 27000-serien, er 31000 en mer generell standard, som ser på risiko som konsept, og ikke forbundet med et fagfelt.

Siden begge utgavene av standardene jeg har omtalt her kom ut, 27000-serien og 31000, jobbes det med å samle terminologien i ISO Guide 73:2009 – Risk Management – Vocabulary [17].

3.1.7 NIST Special Publication 800-39 – Managing Information Security Risk – Organization, Mission, and Information Security View

NIST (National Institute of Standards and Technology), den amerikanske motparten til ISO, har også utviklet en rekke standarder, utgitt som *Special Publications*. Jeg ønsker å belyse de tre mest relevante utgivelsene for min oppgave, nemlig SP 800-39 [44], SP 800-30 [43] og SP 800-37 [45]. Først ser jeg på SP 800-39 [44], som er den mest generelle av utgivelsene. Denne har klare likheter med ISO 27001 [28], ISO 27005 [31] og ISO 31000 [16].

SP 800-39 adresserer risiko på tre nivåer; det øverste nivået – nivå 1 – omhandler risiko for organisasjonen. Nivå 2 ser på forretningskritiske prosesser, og nivå 3 belyser risiko i informasjonssystemer. Toppnivået klassifiseres som strategisk risiko, og nivå 3 beskrives som taktisk risiko. Publikasjonen foreslår også noen generelle virkemidler for å behandle risiko på de forskjellige nivåene. For eksempel foreslås det opprettelsen av *Risk Executive* på organisasjonsnivå, sikkerhetsarkitektur på nivå 2, og risikovurderinger av teknologi på nivå 3.

I kapittel 3 foreslår de forskjellige aktiviteter for å identifisere, vurdere, overvåke og behandle risiko. De første vedleggene til standarden adresserer ord, uttrykk og forkortelser benyttet i standarden. Resten av vedleggene foreslår roller og ansvarsområder, prosessoppgaver i risikohåndtering, strategier for å håndtere risiko, og modeller for ledelse og tillit.

3.1.8 NIST Special Publication 800-30 - Revision 1 – Guide for Conducting Risk Assessments

Denne standarden skal anses som en guide for å utføre risikovurderinger i tråd med SP 800-39 [44]. Her foreslås det at utfallet av en risikovurdering vil påvirkes av organisasjonens risikostrategi, og det nevnes at risiko kan forstås som at "**noen** utfører **noe**, som utnytter en **sårbarhet** – som innehar en rekke **forhåndsbetingelser** – som fører til en **innvirkning** på noe bedriften har". Det tas også høyde for at det finnes uvisshet i alle vurderinger av risiko, da man blant annet ikke kan forutsi fremtiden.

Det er også en del konkrete forslag til hvordan man skal gå frem i en analyse av risiko. Det er stegvis beskrevet hvordan man skal identifisere hensikt, scope, forutsetningene, kildene og risikomodellen til analysen. Videre beskrives det hvordan man skal gjennomføre analysedelen, og hvordan risiko skal formidles til slutt.

Vedleggene tar for seg trusselagenter, sannsynlighetsskalaer, trusselscenarier, sårbarheter, innvirkningsskalaer og lignende.

3.1.9 NIST Special Publication 800-37 - Revision 1 – Guide for Applying the Risk Management Framework to Federal Information Systems – A Security Life Cycle Approach

SP 800-37 [45] kan sees på som en standard for hvordan man skal utføre PDCA, introdusert i 27000-familien. De har delt opp sirkelen noe, men også her tar de høyde for at noe skal planlegges, innføres, vurderes og reageres på. Denne standarden bygger også på SP 800-39. Her blir det i tillegg til å foreslå hvordan man gjør det, listet opp en del milepæler man kan sjekke om man har nådd i prosessen for å implementere et sunt risikohåndteringsrammeverk.

Standardens vedlegg adresserer blant annet roller og ansvarsområder, ledelsesmodeller og strategier for å reagere på risiko.

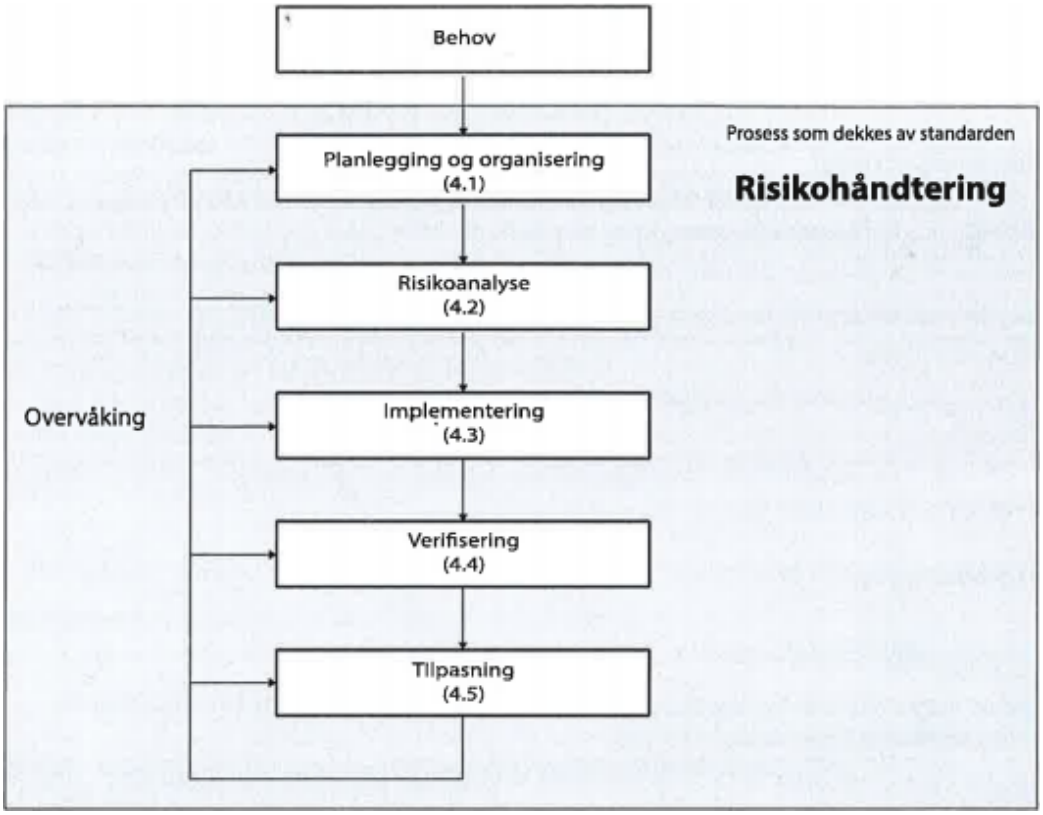
3.1.10 NS5830:2012 Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Terminologi

Organisasjonen Standard Norge har også utviklet en standard for hvordan man bør beskytte seg mot tilsiktede handlinger, altså målrettede angrep. Den første standarden; NS5830:2012 [40] omhandler hovedsakelig hvilke ord og uttrykk man ønsker å forholde seg til.

3.1.11 prNS5831:2013 Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Risikohåndtering

Da denne standarden ikke var publisert på tidspunktet jeg skrev oppgaven, fikk jeg tilsendt et utkast til standard – prNS5831 [41]. Formålet med denne standarden er å fastsette krav til utarbeidelse av prosedyrer for risikohåndtering, og det defineres en prosess for kontinuerlig håndtering av

risiko, se figur 3.4.



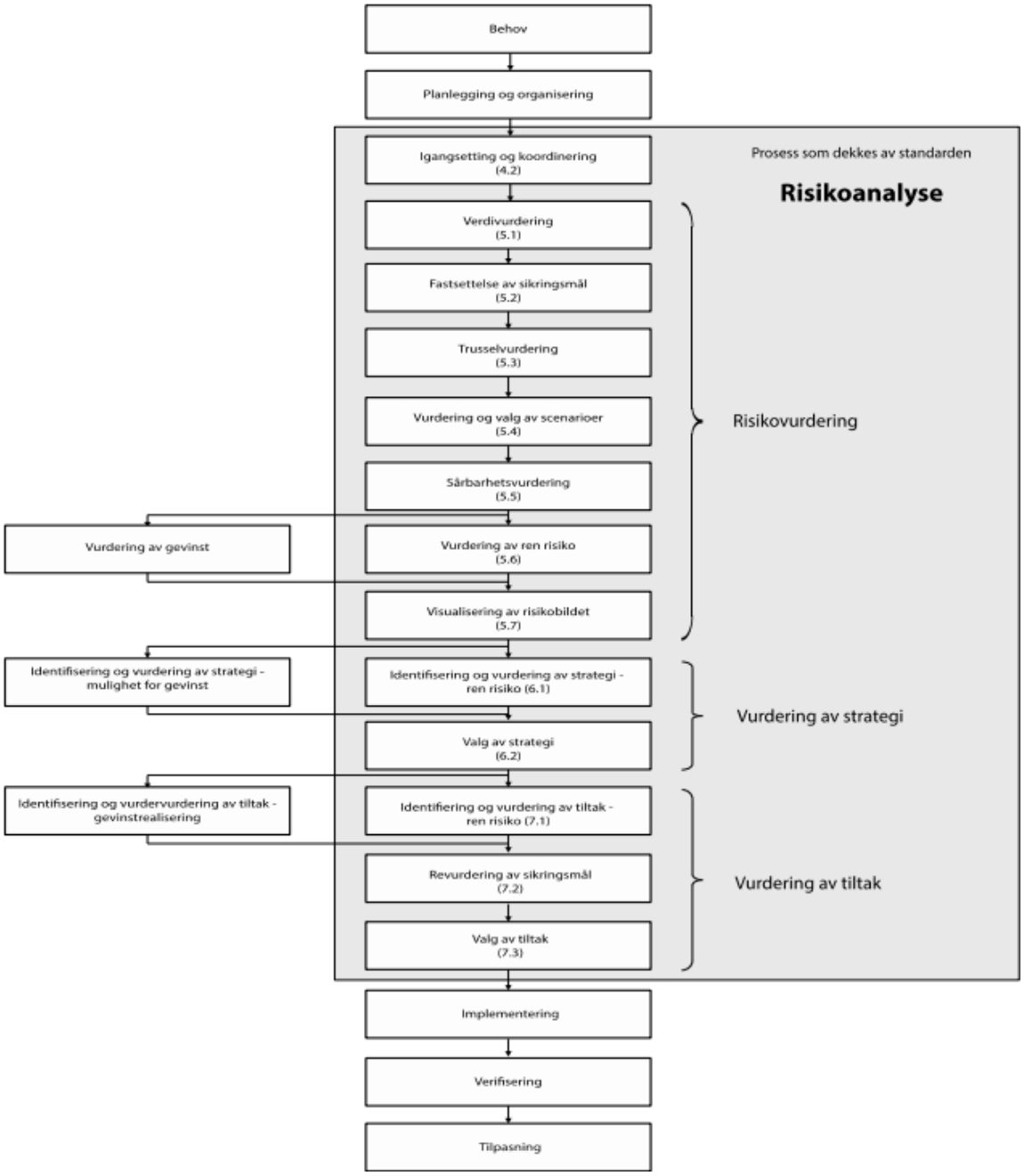
Figur 3.4: Forslag til prosess for å håndtere risiko.

Videre defineres det ytterligere ord og begreper som ikke allerede er nevnt i NS5830, samt at det gjennomgås de ulike stegene beskrevet i tegningen over på en diffus måte. Det er uvisst hva denne standarden tilfører som ikke allerede er nevnt av ISO og NIST.

3.1.12 prNS5832:2013 Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Risikoanalyse

Da Standard Norge heller ikke hadde utgitt denne standarden på tidspunktet for min oppgave, forholder jeg meg også her til et forslag til standard – prNS5832 [42]. Denne standardens formål er å definere metoden for hvordan

man skal utføre en risikovurdering med hensyn til målrettede angrep, og tar med andre ord for seg et helt avsnitt presentert i prNS5831. I likhet med prNS5831 er det også her definert noen steg som bør utføres og hva som skal komme i hvilken rekkefølge, se figur 3.5.



Figur 3.5: Forslag til prosess for å analysere risiko.

Som vi ser i den venstre delen av figur 3.5, er det ikke tatt hensyn til vurdering av muligheter for å tjene penger eller skape verdier, en såkalt positiv risikovurdering. Det presenteres også en klar rettesnor for hvordan analysen skal gjennomføres. Hvert eneste skritt blir også forklart i korte trekk gjennom hele standarden.

Jeg er usikker på om det er en hensiktsmessig rekkefølge på de forskjellige aktivitetene. Det kan virke som at det er uhensiktsmessig å definere trusselagentene før man har definert scenariene. Videre kan det også virke uhensiktsmessig å definere risikoakseptnivå på forhånd. Det kan være en idé å ha gjort seg opp en formening om hva man kan akseptere, men dette må uansett tilpasses det utvidede risikobildet man får mot slutten av en ideell analyse.

3.2 Vitenskapelige kilder

I tillegg til å gå igjennom standardene for å få et inntrykk av hvordan risiko skal forstås, har jeg også basert meg på to bøker av Terje Aven, "Misconceptions of Risk" [5] og "Risk Analysis – Assessing Uncertainties Beyond Expected Values and Probabilities" [4]. Vi skal se nærmere på "Misconceptions of Risk" [5]. Dette er to veldig interessante bøker, hovedsakelig fordi risiko kan være så mangt, og det er viktig å forstå de vanligste fallgruvene for å kunne formidle risiko for en oppdragsgiver på en tilfredsstillende måte. Jeg kommer til å supplere Avens eksempler med mine egne der det passer seg.

3.2.1 Misconceptions of Risk

I den første av bøkene – Misconceptions of Risk – drøfter Aven 19 forskjellige forestillinger av hva risiko er. Det er to grunner til at jeg ønsker å se nærmere på disse forestillingene. Den første grunnen er at Terje Aven har skrevet mange bøker som konsulenter benytter som støttelitteratur for å bedre forstå risiko.

Dernest mener jeg at det er viktig å forstå hva som menes med risiko for å kunne formidle og visualisere risiko i en risikovurdering.

Aven nevner 19 forskjellige forestillinger, eller som han liker å kalle dem, *misoppfatninger* av risiko. Dette er oppfatninger som Aven har kommet over gjennom sitt arbeid med risiko, og mange av dem lever i beste velgående i bransjen idag. Det er viktig å ha et forhold til disse oppfatningene, da de danner grunnlaget for å kommunisere hvor utsatt en organisasjon er for risiko gjennom en risikovurdering. I de følgende avsnittene vil jeg ta for meg disse forestillingene.

Risiko tilsvarer den forventede verdien

Med dette som hypotese beskriver Aven en del scenarier, hvorav ett av scenariene omhandler et spill av typen russisk rulett. Kort fortalt går spillet ut på at man plasserer en - 1 - kule i en seksløper og trekker av. Dersom man treffer kulen taper man 24 millioner, men dersom man **ikke** treffer kulen – vinner man 6 millioner. Summerer man dette, er det $5/6$ sannsynlig at man vinner 6 millioner og $1/6$ sannsynlig at man taper 24 millioner. Skal man regne ut den forventede verdien i dette tilfellet vil man få et regnestykke som ser ut som følgende: Forventet risiko/gevinst = $(-24 \times 1/6) + (6 \times 5/6) = -4 + 5 = 1$. Den forventede risikoen i dette tilfellet blir altså $+1$ million for hver eneste gang man trekker av. Dette hevder Aven at ikke vil gi noe korrekt bilde av risiko, da de fleste mennesker har en aversjon mot risiko. Han mener at det er viktig å se forbi den forventede verdien, og i den forbindelse ta i betraktning den opplevde verdien. For mange vil kanskje ikke verdien av 6 millioner inn på konto være nok til å endre livet til det bedre i noen vesentlig grad, mens å måtte ut med 24 millioner kan drastisk redusere livskvaliteten. For mange er da dette en sjanse de ikke er interesserte i.

Også Bernoulli [7] har skrevet om dette, og illustrerer det med at dersom to menn ville gamblet halvparten av det de eide – forutsatt at de var verdt det samme – på mynt eller kron med en rettferdig mynt, er det veldig få som vil

gå med på dette. Nettopp fordi nytten av økningen i verdi på en halvpart av det man allerede eier, er så veldig mye mindre enn ulempene ved å miste halvparten. Kahneman [33] har tatt for seg Bernoullis teori om forventet verdi, og påpekt at det største hullet i Bernoullis teori, er at det ikke defineres et referansepunkt, og at selv om en forventet verdi kan være lik for to personer, så har man ikke tatt høyde for hvilke forutsetninger deltagerne kommer fra.

Studier [8] viser at folk har en tendens til å være risikosøkende ved lav sannsynlighet, unntatt hvis de står overfor store tap som medfører risikoaversjon (f.eks ved å kjøpe forsikring). Folk vil gjerne akseptere risiko for små eller moderate tap eller å unngå visse eller overveiende sannsynlig store tap. Den siste tilfelle kan illustreres med en situasjon der noen står overfor en umiddelbar høy fare (for eksempel en brann) og må raskt avgjøre hvorvidt man skal bruke en usikker måte (f.eks et skadet tau) for å komme seg ut av denne faren. Folk velger gjerne å bruke denne usikre metoden, og dermed å ta denne høye risikoen, siden det er et bedre alternativ enn døden. Disse studiene viser at risikoholdninger ikke blir bestemt av nyttefunksjonen alene.

Det er imidlertid ikke tilstrekkelig å kunne ta i betraktning sannsynligheter og absolutte verdier. Jøsang og Lo Presti [32] presenterte en risikomodell der relativ andel av total formue brukes for å uttrykke hvor mye man er villig til å tape. To eksempler illustrerer dette.

I det første eksemplet skal en person sette hele sin formue på ti millioner i en enkelt plassering, og velger typisk å sette pengene på en høyrentekonto. Sannsynligheten for suksess er lik sannsynligheten for at pengene vil være trygge i banken, og gevinsten er lik renten. Selv om penger i banken vanligvis er svært trygge, kan de aldri være 100%, så det er en liten mulighet for at de kan gå tapt. Så når hele formuen står på spill har folk risikoaversjon. Det andre eksemplet er å kjøpe et lodd lodd for ti kroner, der sannsynligheten for tap er nær 100%. Der utgjør innsatsen for et vanlig, velstående menneske en ubetydelig del av formuen. Det faktum at folk kjøper lodd med stor sannsynlighet for tap kan forklares med at gleden ved å delta har en verdi

i seg selv. Å kjøpe to lodd vil ikke doble gleden særlig, så folk kjøper som regel få lodd. For et lutfattig menneske i et utviklingsland som kanskje bare har ti kroner, ville det være en uakseptabel risiko å kjøpe lodd, fordi det ville medføre tap av hele formuen med nær 100% sannsynlighet.

Risiko tilsvarer sannsynlighet eller sannsynlighetsfordeling

En annen hypotese han ønsker å bestride er at risiko tilsvarer sannsynlighet eller en sannsynlighetsfordeling for at en ønsket eller uønsket hendelse skal inntreffe. Dette illustreres med et tilsvarende scenario, denne gangen bare med en terning. For å forenkle det hele har han sagt at for hver gang man ruller 6 på terningen, taper man 24.000. Dersom den lander på et hvilket som helst annet tall vinner man 6.000. Altså er sannsynligheten for at man vinner: $\mathrm{P}(gevinst) = 5/6$ og sannsynligheten for at man taper: $\mathrm{P}(tap) = 1/6$. Det finnes derimot en del forutsetninger her for at denne sannsynligheten stemmer. En av forutsetningene er at terningen er rettferdig. Dersom du er sikker på at terningen er fiklet med – enten på bakgrunn av informasjon du har om at terningen ofte er fiklet med, eller at du kjenner personen som tilbyr deg spillet som en kjeltring – stiller selvfølgelig situasjonen seg litt annerledes. Sett at du "*vet*" at han bruker jukseterning i halvparten av spillene, da blir sannsynligheten for å vinne og å tape dramatisk endret. Det er ikke lenger sannsynlig at du vinner dersom du forutsetter det du tror du allerede vet, og risikoen øker. Dette uten at du har fått bekreftet dine egne forutsetninger. Aven mener derfor at risiko aldri kan bevises ved hjelp av sannsynlighet, men at det kan sees på som en indikator på risiko. Uansett hvordan man beregner sannsynlighet vet vi ikke hva som vil skje i fremtiden, og overraskelser kan inntreffe.

Risiko tilsvarer kvantilen for sannsynlighetsdistribusjon (value-at-risk)

Videre er det en oppfatning at risiko utgjør kvantilen for sannsynlighetsdistribusjons, eller 100%-kvantilen. Kort fortalt går denne oppfatningen ut på at man regner ut den siste persentilen, eller 100%-persentilen for at en kostnad overskrider en gitt verdi. Sett at man mener at man er 99% sikker på at tapet blir på ti millioner, så regner man ut den siste persentilen som utgjør kostnader over ti millioner. *VaR* fanger således opp et "*worst case*"-scenario, og vil gi en sannsynlighet for at alt går helt skeis. Problemet med *VaR* er at den ikke sier noe om utgiftene dersom et slikt scenario inntreffer. Derfor kan konsekvensen være så mye verre enn de kalkulerte ti millionene. Denne oppfatningen av risiko benyttes mest innen finans.

Risiko tilsvarer uvisshet

Den neste oppfatningen Aven mener at man har misforstått, er oppfatningen om at risiko utgjør uvissheten. Oppfatningen er at risiko utgjør uvisshet rundt hvorvidt man når et allerede fastsatt og kanskje avtalt mål. Han eksemplifiserer dette ved å illustrere at ingen ville spekulert i aksjer dersom ikke avkastningen var bedre enn å sette pengene på konto. En viktig forutsetning for å bruke dette som målestokk på risiko er derimot at man nettopp har dette referansepunktet som allerede er kjent, eller på forhånd fastslått. For å avgjøre uvissheten rundt et prosjekt tar man altså variansen, som er kvadratroten av standardavviket, for å finne hvor mye man estimerer at resultatet kan avvike fra referansepunktet. Et prosjekt med høy varians er da følgelig mer risikofylt enn et prosjekt med lavere varians. Derimot mener Aven at dette er en for matematisk tilnærming til risiko, da man kan ha to prosjekter; A og B – med sannsynlighetsdistribusjoner for ingen negativ hendelse og en negativ hendelse; (0.5, 0.5) og (0.1, 0.9). Jo nærmere 1 man er, jo større er sannsynligheten for at utfallet inntreffer. Som vi ser er variansen vesentlig større i alternativ A, følgelig vil det være det mest risikofylte prosjektet. Dette stemmer jo egentlig ikke, da prosjekt B nesten er

garantert et negativt utfall, og man derfor heller bør gå for alternativ A.

Videre vil jeg få minne om definisjonen av risiko i ISO Guide 73 [17]; “risk - effect of uncertainty on objectives”.

Risiko tilsvarer en hendelse

Aven hevder også at en vanlig måte å definere risiko på er å definere risiko som en hendelse hvor verdier står på spill. Videre viser han til to definisjoner av Rosa [48, 49] og IRGC [46], som definerer risiko som en hendelse eller konsekvens av en hendelse.

- **Risiko** er en situasjon eller hendelse hvor noe av menneskelig verdi (inkludert mennesker) er på spill og hvor utfallet er usikkert. [48, 49]
- **Risiko** er en uviss konsekvens av en hendelse eller aktivitet relatert til noe med verdi for mennesker. [46]

For å illustrere konseptene tilpasset informasjonssikkerhet, ønsker jeg å fremme følgende utsagn; ved å være tilkoblet internett risikerer du å få skadelig programvare på maskinen din. Som vi ser her passer dette scenariet til begge de tidligere nevnte definisjonene, dette fordi hendelsen “å få skadelig programvare på maskinen” har innvirking på noe av menneskelig verdi – datamaskinen. Aven hevder derfor at det – med en slik tilnærming til risiko – blir meningsløst å snakke om risikoen for å få skadevare sammenlignet med andre risikoer. Det er heller ikke mulig å bedømme hvorvidt risikoen er høy eller lav, og følgelig er den eneste måten å redusere risiko å unngå hendelsen. Derfor må man uttale seg på måter som indikerer at man estimerer eller stipulerer både grad av risiko og uvisshet. Aven hevder også videre at dersom man først skal klassifisere risiko som en hendelse eller konsekvensen av en hendelse, så kan man like gjerne ta med uvisshet og sannsynlighet, siden man allikevel er nødt til å forholde seg til det når man estimerer risikoen for hendelsen. Definisjonene tar heller ikke høyde for at det kan inntreffe positive konsekvenser.

Risiko tilsvarer forventet ulempe

Som vi så i første avsnittet til Aven, ble det foreslått at risiko tilsvarer den forventede verdien. Motsetningen til dette synet er å mene at risiko tilsvarer forventet nedetid, altså i tråd med Bernoullis [7] tanker om at risiko må gjenspeile nyttighet eller funksjonalitet. Mange går også så langt som å hevde at risiko utelukkende er sannsynligheten for en uønsket hendelse, slik som Cambell [10].

Her hevder Aven at alle analyser av risiko også må forholde seg til verdien av en risiko, eventuelt en forventet ulempe ved en konsekvens, og at denne aldri er upåvirket av personlige preferanser. I et resultat hvor nytte blir evaluert, enten negativ eller positiv nytte, vil det alltid være en stor grad av vilkårlighet, og følgelig kan ikke denne definisjonen problemfritt benyttes.

Risiko er begrenset til objektive sannsynligheter

I dette kapittelet tar Aven for seg arbeid fra 1921 utført av Knight [36]. Knight foreslo følgende rammeverk for å avgjøre hva som var risiko og hva som er uvissheter;

- ***A priori*-sannsynlighet:** sannsynlighet utarbeidet basert på *identiske* scenarier med *identiske* forutsetninger.
- ***Statistisk* sannsynlighet:** empirisk evaluering av frekvensen av assosiasjoner mellom predikater. Forskjellen på denne kategoriseringen og *a priori* er at *statistisk sannsynlighet* benyttes der det finnes det minste tvil om man har uttømt alle mulige variabler for å identifisere scenariet som et *identisk* scenario.
- ***Estimater*:** alle scenarier og hendelser hvor det finnes uvisshet. Dette er den formen for sannsynlighet som er vanskeligst og mest upresis.

Knight hevder at det kun er de to første kategoriene som kan omhandle risiko, og at den siste kun kan uttale seg om uvisshet eller *uncertainty*.

Videre mener han at man i de fleste forretningssituasjoner gjerne snakker om estimater, grunnet at det sjelden finnes to identiske bedrifter som står ovenfor to identiske scenarier. Dette er en spennende tankegang, og har ført til en del andre rammeverk for risiko. Man skal uansett ikke lese noe nytt inn i tekstene til Knight, da han hadde andre forutsetninger for å lage sin bok om risiko enn vi har idag. Til syvende og sist er denne oppfatningen av risiko en semantisk diskusjon, da det uansett er viktig å bli enig om forutsetningene før man starter en risikovurdering.

Risiko tilsvarer risikooppfatning

Her ønsker Aven å fokusere på at risiko kan – for mange – beskrives som egen oppfatning av, eller frykt for, risiko. Dette er en irrasjonell oppfatning av risiko, men samtidig fullt forståelig. Aven kommer med følgende eksempel for å illustrere: Dersom du blir tilbudt å kaste terning, og dersom terningen viser 6 må du betale $\$24.000$. Hvis terningen derimot havner på 1 til 5, får du utbetalt $\$6.000$.

Som allerede diskutert i de tidligere kapitlene i boken, er både forventet verdi og sannsynlighet for gevinst; positiv. Derimot er dette faktorer som spiller inn på den menneskelige psyken, og folk tenker at “dette er for godt til å være sant”. Plutselig legger man selv til faktorer som at tilbyder av nevnte spill **må** være en skurk, og du tillegger ham en høy sannsynlighet for å være juksemaker. Forutsatt at han ikke jukser, avviker opplevd risiko mye fra reell risiko, og du tar valg som er irrasjonelle.

En del faktorer som kan spille inn her, er mangel på informasjon, informasjon du allerede besitter, propaganda, begrunnet og ubegrunnet frykt, samt personlige preferanser.

Risiko relaterer utelukkende til negative konsekvenser

Under det neste punktet tar Aven også opp en oppfatning av at risiko utelukkende omhandler negative hendelser. Han illustrerer dette med at risiko er det man løper når man tar sjanser, og gevinst er det man får når risikoene ikke inntreffer. Risiko kommer fra det italienske ordet "*risicare*" som betyr "*å tørre*" [7]. Ut over dette er de vanligste definisjonene i ordbøker også relatert til negative hendelser, så hele diskusjonen blir semantisk og sporer derfor litt av.

Risiko bestemmes av historiske data

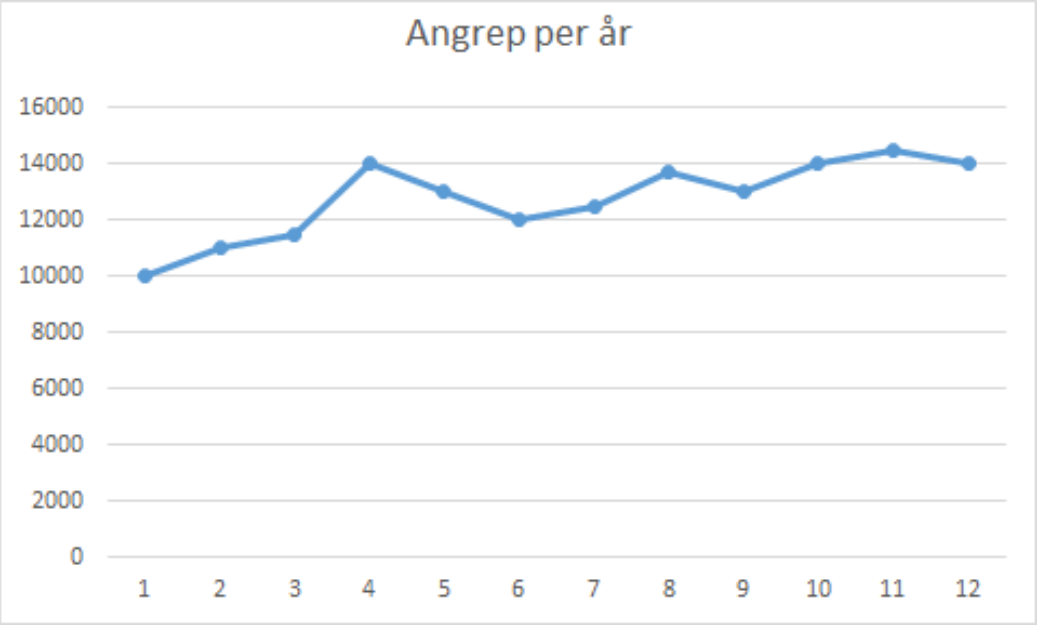
Videre drøfter Aven ideen om at historiske data kan avgjøre risiko. Hovedkonseptet her er at loven om store tall [11] før eller siden vil kunne gi en god indikasjon på fremtiden.

For å illustrere dette kan jeg lage et eksempel der Organisasjon A har dokumentert alle angrepene sine over de siste tolv årene sine. Illustrert i figur 3.6 og tabell 3.7. Som vi kan se får vi med en gang en følelse av hvordan risikoen for å bli angrepet er. Umiddelbart gjør vi oss opp tanker om at trenden de siste årene er en minimal økning, og at det ikke er urealistisk å forvente at man blir angrepet et sted mellom 12.000 og 15.000 ganger neste år.

Tabell 3.7: Angrep per år

År	1	2	3	4	5	6	7	8	9	10	11	12
Angrep	10000	11000	11500	14000	13000	12000	12500	13750	13000	14000	14500	14000

Så; hvorfor er ikke dette en fin måte å spå risiko? For det første kan aldri fortiden *garantere* fremtiden. Derimot kan den gi en kvantifisert indikasjon på hva som vil skje, og loven om store tall vil også sørge for at man – gitt et stort nok utvalg – vil havne omtrent innenfor standardavvikene. En annen faktor



Figur 3.6: Illustrasjon av angrep per år.

man ikke har tatt høyde for når man ser på risiko på denne måten, er at man kan ha målt feil i alle disse årene. Man har ingen garanti for at tallene man baserer risikoutregningen sin på verken er riktige eller presise. Ved innføring av ny teknologi er det mulig at man fanger opp en hel rekke andre angrep som har fløyet under radaren de foregående tolv årene. Det eneste statistikken kan forklare er tendensen i fremtiden, gitt at man benytter seg av samme målemetode og unngår å endre forutsetningene nevneverdig.

Risikovurderinger produserer et objektivt risikobilde

En annen oppfatning er at utfallet av en risikovurdering er en objektiv vurdering av risiko. Dette er selvsagt mulig, gitt at man har strenge og målbare krav for hva som er objektivt. Objektivitet kan da enten beskrives som *a* - resultatenes eksistens uavhengig av revisor eller; *b* - konsensus mellom alle stakeholders. Nå er dette greit i og for seg, men hvis man ikke er klar over fallgruvene i punkt a og b, kan det være lett å ta for god fisk at resultatet av en gitt risikovurdering er objektiv.

Et eksempel der dette er både riktig og uriktig kan være eksemplet jeg illustrerte under forrige punkt. Her er det statistikk som underbygger at generell bruk i organisasjonen tillater et gjennomsnitt på 12770 angrep per år. Man kan ytterligere dele opp dette i for eksempel aldersgrupper og kjønn. Eksempelvis kan man da få en tenkt fordeling som tilsier at dersom du er en mann mellom 20 og 30 år, skal du bli angrepet gjennomsnittlig 3(+/-1) ganger i året. Dersom du er en mann mellom 50 og 60 år derimot, er sannsynligheten for at du blir angrepet 9 ganger, (+/-2) i året. Man kan også finne hvilken angrepsvektor som oftest er vellykket for de forskjellige aldersgruppene. Her kan du derimot godt ha både statistiske avvik og ekstreme topper, enten med mange eller få angrep. Uansett er verken måten man definerer gruppene eller tilegner dem verdier spesielt objektive, og man vil her få et resultat basert på en eller annen persons subjektive forutsetninger.

Det er store iboende uvissheter i risikovurderinger

Misoppfatningen i dette tilfellet går ut på at selve risikovurderingen inneholder stor grad av uvisshet. Dette fordi det finnes bred enighet om at en risikovurdering er en *best effort*-øvelse der man analyserer risiko og uvisshet etter beste evne, uten noen som helst garanti for at funnene kommer til å inntreffe [4]. Paradokset her er jo selvfølgelig at det nettopp er analyseringen av uvisshet som er hovedformålet med en risikovurdering. Det videre spørsmålet er; hvilke uvissheter er iboende? Det dreier seg her om to forskjellige uvissheter.

I en risikovurdering benytter man seg av statistikk og bakgrunnskunnskaper for å analysere uvisshet rundt mulige situasjoner/scenarier. Man benytter seg av loven om store tall og henter ut populasjoner som er tilnærmet like de man skal analysere. Videre forklarer man uvissheten rundt nettopp de gitte scenariene – ikke hvorvidt funnene er garantert å inntreffe. Et eksempel her kan være en analyse av Lotto. I motsetning til en risikovurdering som skal levere visshet, spiller Lotto på nettopp de iboende uvisshetene. I følge Norsk

Tipping [53] er vinnersannsynligheten for vanlig Lotto $1 : 5.379.616$ for førstepremien eller $1 : 138$ for premie i det hele tatt. Alt tatt i betraktning kan man her slå fast med visshet at "*risikoen*" for å vinne førstepremien er så liten at det å spille på Lotto bør frarådes. En enkel kvantifisering og utregning kan også gi deg prisen på alle rekkene du må spille for å være "*garantert*" førstepremien. Det er her uvissheten kommer inn, for du blir aldri garantert noe, men har utsikter til gevinst i følge loven om store tall. Gitt sannsynligheten for førstepremien over, så må du spille omtrent 5.4 millioner rekker, og med en rekkepris på 5 kroner [52] per dags dato, vil dette si at man må "*investere*" $5\mathrm{kr} \times 5.379.616\mathrm{rekker} = 26.898.080\mathrm{kr}$ for å få en tilnærmet sannsynlighet på 100% for å vinne førstepremien. Med mindre du da spiller alle rekkene på samme spill, er du aldri garantert å vinne noe som helst. Når gjennomsnittsutbetalingen på førstepremiepotten er ca 3.7 millioner [51] er ikke dette noe man burde spille på. Men, den iboende uvissheten her er at "*ca 3 personer vinner førstepremien hver uke* [51]", så noe må jo være "galt" med vurderingen vår.

En annen uvisshet som er iboende, er hvorvidt man har identifisert de rette kriteriene, og hvorvidt man har en skjevfordeling som et resultat av fordommer. Dette kan tas høyde for ved å påføre forskjellige kriterier [5]; **'syntaktisk kriterium'**, **'pragmatisk kriterium'**, **'kriterium om kalibrasjon'**, **'heuristikk og fordommer'**, **'evaluering av sakkyndige'** og **'standardisering og konsensus'**. Kort fortalt går disse kriteriene ut på at man finner en tilnærming til uvissheten og påfører den for å akseptere at man ikke kan vite alt. Man må ta høyde for personlige erfaringer og preferanser hos de sakkyndige før man selv velger hva man skal legge vekt på.

Uvisshet i risikomodeller skal kvantifiseres

Ytterligere en oppfatning i risikomiljøet er at *hvis det viser seg at en av modellene man bruker skaper uvisshet, så bør denne kvantifiseres for et bedre overblikk*. Dette er i og for seg en akseptabel tanke, under forutsetning at man hever blikket noe. Dersom modellen skaper uvisshet er det kanskje ikke

den beste modellen å bruke. Aven foreslår å heller forbedre modellen eller velge en annen modell, dersom det reises ytterligere uvisshet etter bruk av risikomodeller. Dette er fornuftig da arbitrær kvantifisering kan skape falsk trygghet mer enn det gir et riktig bilde av situasjonen.

Forøvrig er det i seg selv ikke noe i veien for å kvantifisere, hvis det finnes modeller for kvantifisering av uvisshet. Men, da skal man være sikker på at man ikke gjør det på gal måte.

Det er nyttig å skille mellom stokastisk og epistemisk uvisshet

Mange mener at det er nyttig å skille mellom *a*) **stokastisk uvisshet** som er uvisshet knyttet til tilfeldigheter, og som mange anser som ikke reduserbare, og; *b*) **epistemisk uvisshet** som er knyttet til uvisshet rundt kunnskaper. Eksempler på dette kan være et myntkast, hvor den stokastiske uvissheten går på hvorvidt den havner på kron eller mynt, og den epistemiske uvissheten relateres til hvorvidt mynten er rettferdig, hvorvidt det blåser, et cetera.

Her er det også flere [3, 55, 37] som slutter seg til oppfatningen om at all uvisshet enten kommer som en følge av mangel på informasjon, eller besittelse av informasjon. De hevder det ikke er mulig å kamuflere den sakkyndiges mangel på informasjon under påskudd at det er stokastisk informasjon, og følgelig ikke-reduserbar uvisshet. De lærde strides, og ifølge Aven er det tilsynelatende minoriteten av forskerne som slutter seg til oppfatningen om at all uvisshet er epistemisk som følge av at mangel på kunnskap også klassifiseres som epistemisk. For mange vil det kanskje gjøre en risikovurdering mindre abstrakt hvis man kan skylde på stokastiske variabler.

Bayesiansk analyse er basert på sannsynlighetsmodeller og Bayesiansk oppdatering

Bayes teorem hevder kort fortalt at graden av subjektiv pålitelighet forandrer seg ettersom man blir presentert beviser. Man skulle da tro at en Bayesiansk analyse baserer seg på sannsynlighetsmodeller og Bayesiansk oppdatering, men dette hevder Aven er galt. Å benytte seg av Bayes teorem sammen med sannsynlighetsmodeller er bare fornuftig dersom man kan relatere modellen spesifikt til den Bayesianske oppdateringen. Dersom det blir satt inn en modell med uvisshet eller tall som ikke er relevante, vil man basere oppdateringen sin på gale beviser. Det vil derfor bli følgefeil gjennom hele analysen, og analysen blir verdiløs.

Sensitivitetsanalyser er en type uvisshetsanalyse

Her foreslås det at en analyse av sensitivitet tilsvarer en analyse av uvisshet. En sensitivitetsanalyse har til formål å avdekke hvor utsatt risikoprediksjonen er for avvik. Ideen her er derfor at hvis man avdekker hvor utsatt prediksjonen er for avvik, kan man avgjøre hvilken grad av uvisshet man har for "utfall A" eller "utfall B".

Kort fortalt avgjør en uvisshetsanalyse hvilken grad av uvisshet vi har i analyseresultatene som stammer fra uvisshet i input. Sensitivitetsanalyse derimot, refererer til i hvilken grad uvisshet i input påvirker resultatet av en analyse. Det er noen få, men viktige forskjeller i denne misoppfatningen.

Hovedmålet med en risikovurdering er reduksjon av risiko

For et utrent øre kan det høres ut som om hovedmålet med en risikovurdering er å redusere risiko til et absolutt minstenivå, men her nevner Aven tre eksempler hvor dette tydelig ikke har vært hovedmålet.

1 Romfart

2 Oljeboring

3 Finans

For å illustrere dette raskt, kan vi alle være enige om at et romprogram aldri hadde eksistert dersom man hadde fjernet risikoen for tap av menneskeliv. Det ville videre aldri vært oljeboring hvis man hadde fjernet risikoen for forurensning. Man ville aldri muliggjort investeringer dersom man skulle redusere risikoen for tap av penger – herunder ville aksjer generelt vært en relativt utenkelig deal. En risikovurdering handler om å se på situasjonen og omgivelsene – gjøre en gjennomtenkt og nøye evaluering av dem – samt gjøre seg opp en formening om dette er en risiko man er villig til å akseptere eller ikke. Dersom man ikke er villig til å akseptere risikoen bør man se på virkemidler for å redusere risiko, eventuelt unngå scenariet i sin helhet for å fjerne risikoen helt dersom dette er mulig. Hvis man derimot aksepterer risikoen "*as is*", er det ikke behov for å risikere den noe ytterligere.

Beslutningstagning under uvisshet bør baseres på forskning

Aven mener det er en misoppfatning at beslutningstagning under uvisshet bør baseres på forskning/analyse av situasjonen. Det er to grunnpilarer for et forskningsbasert/analytisk synspunkt. Det ene er at risiko er objektivt for aktiviteten man analyserer, og formålet med en analyse må være å kunne ta fornuftige avgjørelser om hvorvidt risikoen kan aksepteres eller ikke. Den andre pilaren er at dersom risikoen kan godtas, skal den veies mot andre alternativer, slik at man vil finne ut hvor lønnsomt det er å utsette seg for denne, kontra andre akseptable risikoer.

Dette mener Aven er galt, da det vil være for stor grad av uvisshet i et hvert gitt scenario. Ved hjelp av andre analytikere, eller med andre forutsetninger ville kanskje resultatene blitt annerledes, og med dette som utgangspunkt fratar han analysen all troverdighet.

Ved å lene seg for mye på tall avdekket av sikkerhetskonsulenter, vil man trekke seg unna eierskapet til risikoen. Dette er foreslått i en liste fra Fischhoff [14], der han mener man har blitt for naive i forhold til å outsource risikoanalyser.

1. All we have to do is get the numbers right.
2. All we have to do is tell them the numbers.
3. All we have to do is explain them what we mean by the numbers.
4. All we have to do is show them they've accepted similar risks in the past.
5. All we have to do is show them that it's a good deal for them.
6. All we have to do is treat them nice.
7. All we have to do is make them partners.

"Føre var"-prinsippet og risikohåndtering er ikke forenelig

Prinsippet om å være *føre var* defineres på forskjellige måter. *Føre var* skal heller ikke forveksles med *due diligence*, som vi vil forklare litt om senere. De to vanligste måtene er:

- For å beskytte miljøet, skal '*føre var*'-prinsippet benyttes der det er mulig i den grad medlemslandene er i stand til å gjennomføre dette. Hvor det er trusler om seriøs eller ugjenopprettelig skade, skal ikke mangel på full vitenskapelig sikkerhet benyttes for å utsette kostnadseffektive tiltak for å hindre ødeleggelse av miljøet. [1]
- '*Føre var*'-prinsippet er et etisk prinsipp som sier at dersom konsekvensene av en aktivitet kan være seriøse eller innebærer vitenskapelig uvisshet, skal man ta forholdsregler ellers burde aktiviteten unngås. [5]

Den siste definisjonen er den generelle forståelsen av den første definisjonen. Hovedforståelsen er uansett at dersom noe kan få store negative konsekvenser, bør det unngås. Som man har sett av de foregående oppfatningene er utsagnet om at "*føre var*" og risikohåndtering ikke går overens et utsagn som både er treffende og ikke. Grunnen til dette er at man ofte ser på håndtering etter ALARP-prinsippet (As Low As Reasonably Practicable) [9] og en "kost/nytte"-vurdering. I så måte kan man se på "*føre var*" som en forlengelse av *due diligence* og *due care*. Man bør uansett ha et forhold til både prinsippet om å være forsiktig og "føre var"-prinsippet når man gjør en risikovurdering og utvikler en håndteringsplan for risiko. For øvrig bør man ikke ha prinsippet som overordnet mål – da dette vanskeliggjør å drive business på en økonomisk forsvarlig måte.

3.2.2 SANS 20 kritiske virkemidler

I forbindelse med at angrepsscenariene i de forskjellige bransjene er relativt like, har SANS Institute (**S**ysAdmin, **A**udit, **N**etworking and **S**ecurity) utviklet en liste over de 20 mest kritiske virkemidlene for et effektivt cyberforsvar [26]. SANS er en bedrift som spesialiserer seg på opplæring i informasjonssikkerhet og sertifiseringer (GIAC), samt forsking på informasjonssikkerhet. SANS drifter også Internet Storm Center, et prosjekt hvor sikkerhetsspesialister jobber sammen for å overvåke nivået av ondsinnet internettrafikk. Ut ifra denne listen har mnemonic også utarbeidet en liste over trusselscenarier som utnytter de nevnte sårbarhetene som virkemidlene mener å gjøre opp for. I listen under har jeg sitert virkemidlene med fet skrift og forklart hvilke sårbarheter det er meningen at de skal veie opp for.

1 **Liste over autoriserte og uautoriserte enheter**: Kriminelle organisasjoner og nasjoner benytter seg gjerne av automatiserte verktøy som scanner nettverket etter sårbare systemer med tilgang til nettet hos den bedriften de vil angripe. Disse systemene blir så benyttet for å gi tilgang

for angriperen til en senere situasjon. Med en liste over autoriserte enheter vil man lettere fastslå når det har vært uvedkommende på nettet.

2 **Liste over autorisert og uautorisert programvare**: Angripere vil prøve å kompromittere en organisasjons klient slik at de kan benytte seg av den autoriserte klienten i det interne nettet. Dette gjøres ved å installere programvare som vil gi en tredjepart tilganger via den kompromitterte klienten, enten gjennom utdatert "lovlig" programvare eller installasjon av ny, skadelig programvare. Dersom man har bestemt seg for hvilken programvare som kan være installert på bedriftens systemer, vil man oppdage avvik fra dette når det installeres uautorisert programvare.

3 **Trygge konfigurasjoner for maskinvare og programvare på mobile enheter, bærbare maskiner, arbeidsmaskiner og tjenere**: Selv om man har bestemt seg for hvilken programvare som skal være lovlig og ikke, er det fortsatt viktig å sørge for at softwaren er fullstendig oppdatert. Det siste året har det skjedd en vanvittig utnyttelse av Java [13]. Man bør derfor sørge for at man overvåker installert software og sørger for at denne er oppdatert til enhver tid.

4 **Kontinuerlige sårbarhetsvurderinger og utbedring**: Et oppdateringsregime bør håndheves. Man bør hele tiden jobbe med å holde alle aktiva og systemer oppdatert. For å sikre at dette håndheves, bør man hele tiden gjøre vurderinger av sårbarhetsgraden. Dersom man er sårbar bør det iverksettes tiltak for å redusere sårbarheten til et akseptabelt nivå. Dette er arbeid som i stor grad kan automatiseres.

5 **Forsvar mot skadelig kode**: Mye av den skadelige koden som eksekveres er lik i alle organisasjoner, og AntiVirus- og AntiSpyware-programmer er laget for å oppdage de vanligste tilfellene av skadelig kode. AntiMalware-programmer bør derfor installeres på endepunktsklienter for å redusere sårbarheten for ikke-målrettede angrep.

6 **Beskyttelse av applikasjonsprogramvare**: Applikasjoner på nett som tar imot kommandoer fra brukere er veldig utsatt for SQL-angrep, cross-site scripting, clickjacking, buffer overflows og andre ondsinnede injiseringer. Det er derfor viktig at alle applikasjoner, egenutviklede eller innkjøpte, testes for sikkerhetshull og sårbarheter. Enten bør slik testing utføres inhouse, ellers bør det benyttes eksterne verktøy og scannere for å avdekke hullene.

7 **Kontroll på trådløse enheter**: Det forekommer ofte at en angriper kan komme seg til lokasjonen til målet, og ikke trenger å komme seg fysisk inn fordi bedriften sender ut nettet sitt trådløst uten noen som helst form for kontroll eller begrensning på hvem som kan logge på. Det oppdages også fremmede trådløse aksesspunkter som angripere har sneket inn i det interne nettet som en angrepsvektor. Dette bør reduseres og kontrolleres slik at uvedkommende ikke får tilganger de ikke skal ha.

8 **Datagjenoppretningsevne**: Når en maskin først er kompromittert er det mange små endringer som kan utføres på maskinen for at en angriper skal ha tilgang til den. Det er derfor kritisk at man har en god gjenopprettingsrutine for kompromitterte maskiner. Forslag til slik gjenopprettingsrutine er at man har et bilde av en forhåndskonfigurert maskin så man lett kan speile disse. Dette er den eneste måten man virkelig kan være sikker på at man har reversert alle endringene en angriper kan ha gjort på den kompromitterte maskinen.

9 **Evnevurderinger av datasikkerhetskunnskaper og tilstrekkelig trening for å fylle hull i kunnskap**: Enkleste måten å bryte seg inn noe som helst sted må være å bli sluppet inn av dørvakten, og dette vil som regel være førstevalget til enhver angriper under et målrettet angrep. Hele tiden testes brukere, analytikere, utviklere og eiere, og for å unngå å gå fem på er det viktig med ***bevissthets***programmer og godt arbeid hva angår utdanning og retningslinjer. For eksempel lar flere seg lure av

*social engineering*sangrep nettopp fordi de mangler de rette verktøyene for å identifisere en slik svindel.

10 **Trygge konfigurasjoner for nettverksenheter som brannmurer, routere og switcher**: I noen tilfeller krever en organisasjons arbeid at man åpner opp porter i routere, etc, eller at man tillater en type trafikk gjennom brannmuren i en kort periode. Da er det viktig at man i etterkant lukker porter eller sperrer tilganger, slik at et system som i utgangspunktet hadde god sikkerhet, ikke forfaller over tid. Dette er noe angripere er klar over, og de scanner derfor alltid etter dårlig vedlikehold.

11 **Begrensninger og kontroll av nettverksporter, protokoller og tjenester**: I forbindelse med at man konfigurerer en enhet blir det gjerne gjort en vurdering av hva man skal tillate, men det finnes også software som skrur på og muliggjør tjenester man egentlig ikke trenger i samme prosessen. Ofte informeres det heller ikke om at "tilleggstjenester" installeres, og de blir derfor stående gjerne med standardtilkoblinger åpne. Dette vet angripere og prøver seg gjerne med noen standard brukernavn og passord. I tillegg finnes det mye offentlig angrepskode som utnytter standardkonfigurasjoner.

12 **Kontrollert bruk av administrative privilegier**: For en angriper er det vesentlig lettere å kompromittere et system dersom han har administratortilganger, så derfor bør dette begrenses. Det samme gjelder utstrakt distribusjon av påloggingsinformasjon til administratorer. Brukere bør ikke få lov til å kjøre som administratorer som standard, og man bør etterleve sunne passordsrutiner. Hva som er sunne passordsrutiner kan jo selvfølgelig diskuteres [39, 12]. Det bør også identifiseres når det blir lagt til nye brukere til administratorgruppa for å verifisere dette.

13 **Grenseforsvar**: Organisasjoner som har delt inn nettene sine i sikre

og usikre nett, glemmer ofte å segregere og sikre disse nettene. Dette gjør at angripere kan benytte seg av kompromitterte maskiner på usikrede nett som kommuniserer med maskiner på sikre nett, og på denne måten omgå sikringsmekanismene. Det burde derfor settes opp deteksjonsmekanismer for å avdekke korrupte pakker mellom usikrede og sikrede nett.

14 **Vedlikehold, overvåkning og analyse av revisjonslogger**: I mange tilfeller er det eneste beviset for å identifisere et vellykket angrep å finne i logger. Loggene er også det eneste stedet hvor man kan få med seg detaljene i et angrep og hva som har skjedd. Derfor er det viktig å ta vare på loggene og gå igjennom dem med jevne mellomrom. Angripere satser mange ganger på at organisasjonen ikke går igjennom logger selv om de fører dem for revisjonshensyn.

15 **Kontrollert tilgang basert på "*Need to Know*"**: Her er casen at man ikke skiller mellom intern, sensitiv og offentlig informasjon. Alt av informasjon blir oppbevart samme sted med samme rettigheter, og for en angriper er det da veldig lett å hente ut konfidensiell informasjon fra hvilken som helst bruker. Det bør derfor identifiseres når en bruker prøver å få tilganger til informasjon man ikke har tilgang på. På den måten er det mulig å se spor etter kompromitterte brukere som plutselig snoker i klassifisert informasjon, og det vanskeliggjør tilgangen for en angriper dersom han ikke får aksess til rett bruker.

16 **Kontroll og overvåkning av brukerkonti**: Angripere søker hele tiden etter å angripe legitime brukerkontoer som er inaktive. Med dette følger det også et sett med privilegier, uten en bruker som kan følge med på endringer. Kontoene kan for eksempel være for tidligere ansatte, folk som er ansatt i en kort tidsperiode eller andre som skal ha en tidsbegrenset tilgang. Dersom man ikke hele tiden følger med på hvilke kontoer som er i bruk og hvilke som skal være i bruk, kan det ligge

kontoer som senere kan brukes til ondsinnet aktivitet.

17 **Forhindre tap av data**: I tilfeller der angripere har hentet ut store mengder med sensitiv informasjon, er dette gjerne vellykket siden organisasjonen som mister data ikke har noen måte å kontrollere dataflyten ut av nettverket. Her bør man ha en sammensatt kontroll for å redusere datatrafikken ut, enten over nett, gjennom eksterne logiske medier eller fysiske kopier av informasjonen, med automatisk varsling om at data klassifisert som intern eller sensitiv er på avveie og hvem som gjorde det.

18 **"*Incident Response*" og ledelse**: Hva skal man gjøre hvis uhellet først er ute? Dette spørsmålet er det mange organisasjoner som stiller seg uten å ha noe adekvat svar. Skadene kan i ytterste konsekvens være ugjennoprettelige. Det er derfor viktig at man har en gruppering i organisasjonen, eller tilgang på en gruppering som, steg for steg, kan begrense skadene, utrydde angriperens nærvær og gjenopprette status til et sikkert modus.

19 **Trygg nettverksarkitektur**: Alle de tidligere virkemidlene er gode tiltak for å forhindre angrep eller redusere konsekvensene av et vellykket angrep. Alt dette er forøvrig forgjeves dersom ikke infrastrukturen er robust eller grundig sikret. Med dårlig arkitektur er det fortsatt mulig å misbruke sårbarheter. Det er derfor like viktig å designe nettverket sitt på en solid måte som å implementere virkemidler mot sårbarheter.

20 **Penetrasjonstester og "*Red Team*"-øvelser**: Det er også viktig å ha et forhold til sikkerhet, og jevnlig kjøre tester av systemet. Hvis man ikke har kontroll på hva som skjer når man først har kommet igjennom forsvarsmekanismene, er det også vanskelig å gjøre noe med det. Ved testing er det også mulig å finne "*murens svakeste punkt*", slik at man kan gjøre noe med det. En penetrasjonstest gir som regel også mer

detaljer rundt en sårbarhet enn en risiko- og sårbarhetsanalyse vil gjøre. Ved å foreta gode tester på sin egen organisasjon, vil man også avdekke svakheter i alle ledd, fra det tekniske og retningslinjer, til kunnskaper og rutiner for reaksjoner.

For å oppsummere SANS' kritiske virkemidler er det også laget en handlingsplan for å sikre seg mot det groveste av angrep. Denne handlingsplanen legger til grunn at man sammenligner status i sin egen organisasjon opp mot de foreslåtte virkemidlene og avgjør hvor mange avvik man har. Videre har SANS foreslått hva som er umiddelbare fordeler ved innføring av virkemidlene. De mest kritiske burde selvfølgelig implementeres momentant. Øvrige kontroller innføres over tid, for å sikre en sunn holdning og forståelse av hvorfor man implementerer virkemidler som *kan* redusere funksjonalitet. De australske myndighetene har laget en tilsvarende liste over strategier for å begrense skadene og omfanget av målrettede cyberangrep [2].

3.3 Terminologi og begreper

I forbindelse med at fagområdet er generelt, ønsker jeg å belyse de to begrepene ***risiko*** og ***informasjonssikkerhet***. Grunnen til dette er først og fremst å illustrere begrepenes mange betydninger. I tillegg til at risiko allerede defineres i standarden, finnes det også mange definisjoner som beskriver risiko på en vel så presis måte som ISO 27000-serien.

- **Risiko** er sannsynligheten for en uønsket hendelse [10]
- **Risiko** er sannsynligheten for et ugunstig utfall [25]
- **Risiko** er et mål på sannsynlighet og alvorlighetsgrad av ugunstige effekter [38]
- **Risiko** er kombinasjonen av sannsynlighet for en hendelse og konsekvensen av denne [31]

- **Risiko** er sannsynligheten og konsekvensen, mer spesifikt er risiko tripletten (s_i, p_i, c_i) hvor s_i er et scenario, p_i er sannsynligheten for s_i og c_i er konsekvensen av det *i*-te scenariet, *i* = 1, 2 ..., *N*. [34, 35]

- **Risiko** er potensialet en valgt handling eller aktivitet (inkludert å forholde seg inaktiv) har for å føre til et tap (et uønsket utfall). Potensielle tap i seg selv kan også defineres som **risiko** [54].

- **Risiko** er en situasjon eller hendelse hvor noe av menneskelig verdi (inkludert mennesker) er på spill og hvor utfallet er usikkert. [48, 49]

- **Risiko** er en usikker konsekvens av en hendelse eller aktivitet relatert til noe med verdi for mennesker. [46]

- **Risiko** refererer til uvissheten rundt og alvorlighetsgraden av konsekvensene (eller utfallene) av en aktivitet relatert til noe mennesker setter pris på. [6]

- **Risiko** er en situasjon som involverer utsettelse for fare. Synonymer; fare, våge, sjanse. [22]

Som vi kan se er dette alle definisjoner man har brukt tid på å utvikle, og alle kan både forsvares og relateres til informasjonsteknologi. Jeg ønsker ikke å ta stilling til hvilken av definisjonene som er den riktigste, og kommer til å sentrere min videre diskusjon rundt problemet med å definere risiko på en god måte.

Videre ønsker jeg å se på ordet **informasjonssikkerhet**. På norsk brukes hovedsakelig ordet *sikkerhet* når det diskuteres informasjonssikkerhet, selv om man på engelsk gjerne sjonglerer mellom *security* (sikkerhet), *safety* (trygghet), *certainty* (visshet) og *assurance* (forsikring). Dette kunne man gjerne gjort i det norske miljøet også, da det blir levert forskjellige tjenester innenfor '*sikkerhet*' som i realiteten ikke nødvendigvis utgjør det samme. For å illustrere dette ønsker jeg å komme med de engelske definisjonene [21, 23, 20, 24] på de fire foregående ordene:

Security

- The state of being free from danger or threat.
- The safety of a state or organization against criminal activity such as terrorism, theft, or espionage: “national security”.
- **Synonyms:** safety - surety - guarantee - safeguard - bail - guaranty

Safety

- The condition of being protected from or unlikely to cause danger, risk, or injury: “they should leave for their own safety”.
- Denoting something designed to prevent injury or damage: “a safety barrier”; “a safety helmet”.
- **Synonyms:** security - safeness

Certainty

- Firm conviction that something is the case.
- The quality of being reliably true: “a bewildering lack of certainty in the law”.
- **Synonyms:** certitude - assurance - sureness - surety

Assurance

- A positive declaration intended to give confidence; a promise: “he gave an assurance that work would not recommence until Wednesday”.
- Confidence or certainty in one’s own abilities: “she drove with assurance”.

- **Synonyms:** security - certainty - insurance - surety - assuredness

Som vi ser er alle ordene her transitivt synonyme, da alle ordene har ett eller flere av de andre ordene som synonymer. Jeg synes dette beskriver feltet *informasjonssikkerhet* på en passende måte, da hovedmålet med sikkerhetsbransjen er å levere en visshet om at man er sikret mot "*det skumle*". Dette gjøres kanskje best ved å forsikre kunden (gjennom leveranser) om at han kan være trygg på at han har den beste sikringen.

Det ble av Aven [5] også introdusert et prinsipp om å være føre var, samt et prinsipp om å "se før du hopper". Da disse prinsippene samsvarer litt med *due diligence*, synes jeg det er greit å se på hva som menes med *due diligence*. Her har Jacques Richardson [47] skrevet en artikkel som ser på det å spå fremtiden med de to forskjellige prinsippene; due diligence og føre var, og hvilke konsekvenser mangel på fremsikt kan få. Hovedforskjellen mellom '*føre var*' og '*due diligence*' kan oppsummeres på følgende måte:

- **Due diligence**: At man har tatt nødvendige forholdsregler slik at man kan reagere i tilfelle uventede situasjoner skulle oppstå.
- **Føre var**: Dersom ikke noe er en absolutt nødvendighet, prøv å unngå situasjonen i sin helhet.

Personlig ønsker jeg å se på *due diligence* som forholdsregler det er rimelig å forvente at man har tatt, og *føre var* som forholdsregler som går godt ut over det man kan forventes å gjennomføre; for eksempel å unngå aktiviteten helt.

3.4 Oppsummering som gjenspeiler forskningsspørsmålene

I dette kapittelet har jeg prøvd å besvare og belyse en rekke av arbeidsspørsmålene mine (se 1.2.1). Helt konkret har jeg tatt opp momenter som har besvart eller belyst følgende spørsmål:

1. ***Hvordan påvirkes risikoarbeid i en organisasjon av risikoforståelsen?***

    1.1 Hva er "**risiko**"?

    1.3 Hvordan kan risiko forstås

    1.5 Hvordan måles risiko?

        - Hvem definerer metrikkene?
        - Hvordan defineres metrikkene?

    1.6 Hvem har nytte av en slik masteroppgave om risikovurdering?

2. ***Hva er forutsetningen for et vellykket risikoarbeid i en organisasjon?***

    2.1 Hva er "**risiko**"?

    2.2 Hva er "**informasjonssikkerhet**"?

    2.4 Hvem foretar risikovurderinger?

    2.5 Hva er formålet med en risikovurdering?

3. ***Hvordan kan aktivitetene og resultatene i ISO 27005 formaliseres?***

    3.2 Hva er formålet med ISO 27000-familien?

    3.3 Finnes det alternativer til ISO 27000-familien?

Jeg har ved gjennomgang av standardene gitt vinklinger på hva risiko er, hvordan det kan forstås og hvordan det måles. Det er også illustrert hvem som er innenfor målgruppen til standardene, og følgelig også hvem som kan ha bruk for denne oppgaven.

Jeg har ved å inkludere NISTs *Special Publications* [43, 45, 44] og NS5830-serien [40, 41, 42] illustrert at det finnes alternativer til ISO-serien [27, 28, 29, 30, 31], og også alternativer til hvordan risiko skal ansees og behandles. Dette har vært med på å også belyse hvordan risiko bør forstås og hva det vil si å utsettes for risiko i informasjonssikkerhetsøyemed.

Avens bok om misoppfatninger [5] og SANS liste over de 20 mest effektive virkemidlene [26] har hjulpet til å begrunne hvordan risiko burde forstås og måles. Min gjennomgang av definisjonene av *risiko*, *informasjonssikkerhet* og *sikkerhet* har også vært med på å avklare hva jeg legger til grunn for resten av diskusjonen min.

KAPITTEL 4

Erfaringer

I dette kapittelet tar jeg for meg tre forskjellige caser. Alle casene er – som nevnt tidligere – reelle caser, erfart av mnemonic AS. Da jeg ikke har mulighet til å gå ut med navn, er disse anonymisert, og alt som kan avsløre hvor de forskjellige risikoanalysene er utført er fjernet eller endret til en mer generell beskrivelse. Begrunnelsen for dette er taushetserklæringer som jeg har undertegnet i kraft av mitt ansettelsesforhold.

Årsaken til at jeg har valgt å se på de følgende casene, henger direkte sammen med hovedspørsmålene mine (se 1.2.1). For det første ønsker jeg å avdekke hvordan risiko defineres, og hvordan de omtalte bedriftenes risikoforståelse påvirker risikoarbeidet. For det andre er det viktig for meg å kunne se på hvordan ISO 27005 [31] benyttes av konsulenter hos kunder. Dette vil gi meg viktig informasjon for å senere kunne uttale meg om hvordan aktivitetene og resultatene i standarden kan formaliseres. For det tredje ønsker jeg å se om det er forskjeller hos de tre organisasjonene som kan indikere noe om nødvendige forutsetninger for vellykket risikohåndteringsarbeid. Dette vil også gi meg nyttig informasjon til diskusjonen i kapittel 5.

4.1 Offentlig organisasjon

I den første casen er det utført en risikoanalyse hos en større offentlig organisasjon. Forutsetningene er at organisasjonen har jobbet med informasjonssikkerhet mellom 10 og 20 år, og utfører jevnlig risikoanalyser av de mest kritiske systemene. Det indikeres fra konsulenten at det er også tradisjon for å iverksette tiltak for å følge opp avvik og funn, samt at organisasjonens direktør blir forelagt de viktigste funnene. Resultatet fra risikoanalyser inngår i den sentrale handlingsplanen til organisasjonen.

I denne organisasjonen var mnemonics mandat å gjennomføre en risiko- og sårbarhetsanalyse (*RoS-analyse)* på følgende elementer: **epostsystemene**, **diverse interne portaler**, **dokumentlagre**, **mobile enheter**, **interne forretningsprosesser/-verktøy** og **infrastruktur og arbeid med informasjonssikkerhet**. Under disse områdene ble det også definert problemstillinger som skulle analyseres. Alt dette ble dokumentert i et underskrevet mandat-dokument der sjefen for organisasjonens IT-avdeling er oppdragsgiver. Her ble det også definert hvilke krav og mål som skal være oppfylt før man kan anse RoS-analysen som fullført, samtidig defineres det også hva som IKKE inkluderes i analysen.

Det ble avholdt et oppstartmøte, og på dette møtet ble det definert et mandat for RoS-analysen, dokumentgjennomgang, workshop og intervjuer. Kunden forpliktet seg også til å stille med ressurser og mannskap i tide og etter behov. I prosessen ble det også avtalt at det skulle benyttes ISO 27005 [31] som rammeverk for analysen.

Videre skulle det settes av tid til å analysere dokumenter, herunder dokumenter som beskrev de ansattes oppførsel, en såkalt "*brukerinstruks*". Videre ble det analysert alt av dokumentasjon angående systemene som skulle analyseres. Hadde det eksistert en sikkerhetspolicy ville denne også blitt analysert. En analyse vil her si at man går igjennom all dokumentasjonen som kommer inn, avdekker avvik mellom sikkerhetspolicy og dokumentasjo-

nen. Hvis det ikke foreligger en sikkerhetspolicy, bør det sammenlignes avvik mellom "*best practice*" eller anbefalt practice og dokumentasjonen. Her er det kritisk at man får nok dokumentasjon. Det er også viktig at man får den rette dokumentasjonen, og hvis noen velger bevisst å tilbakeholde informasjon, vil dette påvirke resultatet av analysen. Alt man observerer her vil registreres som funn, enten i form av manglende informasjon eller gal dokumentasjon.

Når man skal analysere dokumentasjon av systemer, ser man på hvilke andre systemer systemet snakker med, hvem som har tilganger, hvilke tilganger de har, hvor systemet står, om det er beskyttet, og så videre. Alt som kan sees på som en potensiell trussel skal avdekkes ved hjelp av analysen.

Forøvrig, når det kommer til analyse av brukerveiledninger, policy og andre styringsdokumenter, er det vanlig å se på dekningsområdet til dokumentet. Er det et dokument som søker å dekke behovene i 27000-serien, sjekkes det at den faktisk er i samsvar med standarden. Skal dokumentet derimot beskrive hva som er *akseptabel bruk* i en organisasjon, ser man på innholdet i dokumentet. Her må man som fagperson gjøre kvalifiserte vurderinger av innholdet. For eksempel: hvis det står at man bør patche 1 gang i halvåret, kan man eventuelt registrere avvik hvis man mener at dette er dårlig sikkerhetspraksis og bør forbedres. Det er ellers viktig å se på at retningslinjene ikke bryter med lover og regler.

Da bedriften ikke hadde behov for workshop i denne runden ble det kun avholdt intervjuer. Til disse intervjuene ble følgende grupperinger intervjuet:

- Direktøren
- 3 avdelingsdirektører, IT-sjefen inkludert
- Tjenesteeiere
- Tjenesteansvarlig
- Driftsansvarlig

- Vanlige brukere

Grunnen til at det var disse menneskene som ble identifisert er at direktøren og ledelsen har en god oversikt over hva som er kritisk for forretningen. Driftsansvarlige, tjenesteeiere og -ansvarlige har inngående kjennskap til systemene. Vanlige brukere kan fortelle om hvordan de opplever systemene.

Det er gjerne vanlig å sette av tid samtidig med intervjuene til analyse av informasjonen man får, det ble det også gjort i dette tilfellet. Jeg vil ikke gå inn på spesifikke detaljer rundt hva som ble oppdaget eller hvordan prosessen med analyse ble utført, da dette er sensitiv informasjon.

4.1.1 Funn fra offentlig organisasjon

I denne casen ble det oppdaget og erfart en rekke funn, og som man kan se av Appendix A (kap. A), har jeg intervjuet de ansvarlige konsulentene. Sett bort ifra den faktiske gjennomføringen som kunden fikk, har jeg sett på *hvordan* det var å utføre analysen. Det var ikke interessant for meg å avdekke hvorvidt organisasjonen var sårbar for trussel A eller trussel B. Det var aktuelt for meg å avdekke i hvilken grad ISO 27005 [31] kunne fungere som rammeverk for analysen. Jeg ønsket derfor å avdekke i hvilken grad organisasjonen var ***motivert***, ***moden*** og ***dedikert*** til oppgaven (se forøvrig avsnitt 1.2.1).

Først og fremst ønsket jeg å kartlegge bakgrunnen for at risiko- og sårbarhetsanalysen ble utført, og hva slags kultur de hadde for sikkerhet i organisasjonen. I den forbindelse fikk jeg vite at organisasjonen ikke hadde noen forhåndsdefinert sikkerhetspolicy. Konsekvensene av det er at de heller ikke hadde forhåndsdefinerte risikoakseptansenivåer. Dette meldte det seg et behov for underveis i analysen, og det ble sett på som en ulempe at de ikke hadde forhåndsdefinerte nivåer. Forøvrig hadde de jobbet med risikoanalyser med 2-årsintervaller det siste tiåret, hvilket indikerte en viss dedikasjon og seriøsitet fra organisasjonens side. Konsulentene fikk imidlertid inntrykk av at

organisasjonen kun gjennomførte risikoanalyser for å være i samsvar med god praksis på feltet.

Selv om de fleste var motiverte for å gjennomføre risikovurderingen, var det en generell holdning mot å initiere prosjekter som kunne føre til mer arbeid for de involverte. Dette ble tydeligere underveis i risikoanalysen, da personen med ansvar for oppfølging og implementering av vedtak på driftsiden utviste noe motvilje. Vi antar at han allerede hadde nok arbeidsoppgaver for å fylle dagen, og så kanskje på funnene som personlige angrep på hvordan han utførte sin jobb. Det var faglige uenigheter mellom konsulenten som rapporterte funnene og driftsansvarlig, som resulterte i at driftsansvarlig avfeide enkelte funn som irrelevante.

Det ble tidlig observert at de ansatte hadde veldig god kunnskap om sine forretningsprosesser, mens den generelle kunnskapen om informasjonssikkerhet var heller beskjeden. Det var også mange spesialister, og få som hadde det store helhetsbildet på hvordan ting hang sammen. Man kan spekulere i om dette skyldtes mangel på policy og retningslinjer hva angikk informasjonssikkerhet.

På spørsmål om konsulentene benyttet seg av ISO 27005 som rammeverk, var svaret at det i større grad nå enn tidligere var 27005-tankegang. Konsulentene hevdet derimot at 27005 ikke var noe man benyttet *aktivt*, men at man hadde det i bakhodet under gjennomføringen av en risikoanalyse. mnemonic har utviklet en fremgangsmåte som støtter seg på flere standarder, hvor blant annet ISO 27005 [31] er vektlagt. De støttet seg blant annet også på rammeverk utarbeidet av *Intel Corporation* for å definere trusselagenter [50]. Det ble også lagt vekt på egne erfaringer fra tidligere risikoanalyser, og til å definere trusselscenarier, ble det benyttet SANS [26] liste over 20 mest kritiske kontroller sammen med konsulentenes egne kunnskaper. Disse kontrollene er utviklet for å redusere risikoen fra de vanligste trusselscenariene relatert til informasjonssikkerhet, og fungerer i så måte som et supplement til scenarier man selv måtte definere.

For å måle risiko, ble det i dette tilfellet definert en endelig matrise med 3x3 trinn. Metrikkene som ble benyttet var kvalitativ med trinnene; *Lav*, *Middels* og *Høy*. Dette fordi det ikke er hensiktsmessig å sette arbitrære tall uten noen som helst form for bakgrunn. Aksene i matrisen bestod av *sannsynlighet* og *konsekvens*. Her ble det avtalt på forhånd hva som skal avgjøre sannsynlighetsgraden og konsekvensgraden.

Sannsynligheten kan deles inn i de tre følgende matrisene:

Tabell 4.1: Bevisste handlinger/angrep

Sannsynlighet	Høy	Middels	Lav
Beskrivelse	• Sterkt motivert • God kunnskap • Ingen effektive kontroller for å forhindre utnyttelse	• Motivert • Tilstrekkelig kunnskap • Finnes kontroller som kan forhindre utnyttelse	• Liten motivasjon • Noe kunnskap • Kontroller implementert som vanskeliggjør eller avverger angrep

Tabell 4.2: Ubevisste handlinger/uhell

Sannsynlighet	Høy	Middels	Lav
Beskrivelse	• Lav kunnskap • Få kontroller for å forhindre uhell • Uhell har skjedd flere ganger	• Noe kunnskap • Finnes kontroller som kan forhindre uhell • Uhell har skjedd	• God kunnskap • Gode kontroller for å forhindre uhell • Uhell har ikke tidligere skjedd

Tabell 4.3: Miljøhendelser

Sannsynlighet	Høy	Middels	Lav
Beskrivelse	• Få eller ingen kontroller for å beskytte mot miljømessige trusler • Ulykker har skjedd tidligere	• Kontroller finnes, men har betydelige svakheter • Nestenulykker har forekommet	• Gode kontroller finnes • Nestenulykker har ikke forekommet

Som vi ser er ikke matrisen bygd opp med den klassiske $P(\mathrm{angrep}) = 1 - P(\overline{\mathrm{angrep}})$-oppfatningen av sannsynlighet. Sannsynligheten her er heller basert på i hvilken grad man *anser* trusselagenten eller miljøet å være motivert eller skadelig. Dette sett opp mot hverandre, vil avgjøre en sannsynlighetsgrad man kan kombinere med konsekvens for å få en risikograd.

På forespørsel om konsulenten opplevde at organisasjonen hadde lært noe av risikoanalysen ut over de faktiske resultatene av analysen, eller om de hadde endret graden av modenhet, forklarte konsulenten at hennes erfaring var at organisasjonen hadde lært hva som var viktig i en risikoanalyse. Derimot var det ikke noen endring i innstilling til behovet for risikoanalyse. Etter analysen anså de fortsatt risikoanalyser som et nødvendig onde som man "bare må få gjort unna hvert 2. år".

4.2 Finansinstitusjon

I case nummer to er det utført en risikoanalyse hos en stor aktør i finansverdenen. Forutsetningen her var at organisasjonen allerede har en egen risikoavdeling, men denne avdelingen behandler kun forretningsrisiko. Risikovurderingen av informasjonssikkerheten ble satt bort til eksterne konsulenter, i dette tilfellet; mnemonic. Organisasjonen har med andre ord et forhåndsdefinert forhold til risiko og analyse av dette. I motsetning til den offentlige institusjonen

diskutert i kapittel 4.1, handler denne organisasjonen inn tjenester, prosesser og verktøy fra tjenesteleverandører, og mnemonic ble hyret for å analysere sikkerheten og graden av risiko hos tjenesteleverandørene.

I forbindelse med risikoanalysene hos denne organisasjonen blir det også gjort en konsekvensanalyse for organisasjonen, så man vet hva man er redd for. Dette kan da samkjøres med hva tjenesteleverandørene leverer, og man har i utgangspunktet en klar målsetning med analysen. Derimot er det her vanskelig å få tak i de rette personene tidlig i prosessen, gjerne av flere grunner. En av hovedgrunnene til at det er vanskelig å få med seg de rette personene er at man ikke kommuniserer godt nok til å få med kritisk personell. Dette vil variere fra sak til sak. Det er vesentlig mer kritisk å ha med ledelsen på prestisjeprosjektene enn det er å få med ledelsen på de mer "trivielle" gjennomgangene.

Som i den tidligere casen ble det gjennomført en dokumentanalyse. Her går man igjennom avtalen man har med kunden i forkant av revisjonen. Det etterlyses også dokumentasjon fra tjenesteleverandøren, og det ble sendt ut et "*selvevalueringsskjema*" til dem. Formålet med evalueringsskjemaet er at tjenesteleverandøren får forklare i prosa rundt den tekniske løsningen og at de skal svare på helt konkrete sikkerhetsspørsmål. Dette vil gi konsulentene så mye informasjon som mulig, hvilket igjen sikrer at konsulentene er tilstrekkelig forberedt.

Hos denne kunden ble det i den aktuelle saken avholdt to forskjellige typer intervjuer, Business Impact-intervjuer hos organisasjonen og onsite-intervjuer hos leverandøren.

I konsekvensanalysen velger organisasjonen selv hvem de vil at skal delta på intervjuer (både hvilke individer og hvilke stillinger), basert på anbefalinger fra konsulent. Dette skjer etter at ledelsen og konsulentene har diskutert seg igjennom mulige interessenter. Her er det viktig at organisasjonens medlemmer faktisk innehar kompetanse til å uttale seg om organisasjonens forretningsverdier og har eierskap til risiko. Disse intervjuene blir så utført i

dialogform der det stilles åpne spørsmål hvor hensikten er å få interessentene til å selv nevne hva som er kritisk og ikke. Utformingen av spørsmålene baserer seg på intern dokumentasjon utformet av mnemonic.

Onsite-intervjuene foregår litt på samme måte, men her blir intervjuobjektene plukket ut av leverandøren. mnemonic indikerer hvilke roller de trenger å intervjue, og forhåpentligvis dukker disse rollene opp. Det finnes eksempler der mnemonic har etterspurt spesifikke roller, og helt andre personer har dukket opp. Her er det ofte samsvar med 27002 som er hovedmålet å avdekke, men også hvor utsatt de forskjellige tjenestene tjenesteleverandørene tilbyr er. De vanligste rollene som intervjues hos tjenesteleverandører er:

- Sikkerhetsansvarlig
- Risk manager
- Nettverksarkitekt
- Systemadministratorer
- Fysisk sikkerhetsansvarlig

Det viktigste er at intervjuobjektene får snakke fritt, og at ikke intervjuene foretas som en revisjon. Det blir gjerne gravd i kunnskapshull og andre mangler som kan indikere sårbarheter i systemene. Dette er en bevisst strategi, da empiri tilsier at mange "øver seg" på å unngå uheldige svar dersom det blir mye fokus på spørsmål og svar. Det benyttes her en liste over spesifikke problemområder tilpasset intervjuobjektets rolle i organisasjonen. Denne listen er basert på arbeid fra SANS.

4.2.1 Funn fra Finansinstitusjon

Også i denne casen intervjuet jeg den ansvarlige konsulenten, og siden det heller ikke her er aktuelt å avsløre innholdet i risikoanalysen, men heller fremgangsmåte, er svarene som er avgitt konsulentens egne vurderinger

av situasjonen. Også her har det vært av interesse for meg å avdekke organisasjonens ***motivasjon***, ***modenhet*** og ***dedikasjon***; samt å se på i hvilken grad man har benyttet seg av ISO 27005 i forbindelse med risikoanalysen.

For det første er ikke denne casen samme type case som den forrige casen, og man kan følgelig ikke måle modenhet helt på den samme måten. Eksempelvis har denne bedriften rutiner på at det foretas en vurdering av alle tjenesteleverandører når man skal kjøpe inn tjenester, uansett om det er en stor eller liten tjeneste/komponent. Dette er ufravikelig og akseptert. Forøvrig er det ikke alle tjenester som krever en like grundig vurdering, eller; analyse – noen ganger holder det med en "self assessment" fra leverandøren. Denne ble så i etterkant gått igjennom av mnemonic for å identifisere logiske brister og hull. Denne vurderingen foretas som due diligence.

Det er også en egen risikoavdeling i organisasjonen som til enhver tid jobber med å analysere forretningsrisiko. Videre er toppledelsen involvert i hele prosessen der det er nødvendig, gjerne ved at de blir invitert med på intervjuene med tjenesteleverandøren som skal analyseres. Der det ikke er nødvendig med toppledelsens meninger, henter man inn vurderinger og rapporter som har blitt foretatt tidligere i lignende saker der toppledelsen har gitt generelle retningslinjer. Det foreligger tydelige indikasjoner på at bedriften har en god modenhet når man ser på forholdet til risikohåndtering. De ansatte besitter også en formidabel spisskompetanse. Alle ansatte har god kontroll på sitt eget område og sine egne prosesser. De som trenger å ha kunnskaper om sikkerhet, har dette. Siden de ansatte til enhver tid jobber med risiko er dette noe de har et forhold til og kan dermed relatere til IT-risiko. Det generelle "**awareness**"-miljøet og -kulturen er godt innarbeidet i organisasjonen.

Forøvrig ble det observert at de vanlige brukerne hadde vekslende innstilling til risikoanalysen. De så veldig pragmatisk på øvelsen; selv om de aksepterte og forstod at den skulle gjøres, kunne de tilbakeholde informasjon som resulterte i at deres ønsker ble nedprioritert. Dersom det var en

funksjonalitet de selv hadde etterspurt som skulle analyseres, mente mange at risikoanalysen kunne "**komme i veien for**" selve funksjonaliteten denne tjenesten kunne tilføre. Svarene de involverte ga til utførende konsulent, var selvfølgelig farget av denne frykten og kunne ha innvirkning på resultatet av analysen.

Dette er et aspekt mnemonic har brukt tid på. mnemonic har implementert en forsikring av kunden om at de ikke er partiske, og at de kun ser på sårbarheter opp mot hvilke forretningsverdier organisasjonen selv anser som kritiske. Selv om dette ikke er like akseptert gjennom hele organisasjonen, gjør dette det mye lettere å utføre en risikoanalyse. Det er på forhånd definert hva man kan akseptere, og hva man ikke kan akseptere. På denne måten er det lettere å definere spesifikke scenarier, og det er også lettere å være uttømmende hva gjelder trusler.

Når det kommer til scenarier, ble disse utarbeidet i fellesskap med organisasjonen under konsekvensanalysen. Det ble også tatt ibruk scenarier basert på SANS [26] mest kritiske kontroller. Disse kontrollene beskriver som nevnt en angrepsvektor, og hvordan man kan redusere konsekvensene av denne. mnemonic som bedrift har blitt kjent med denne organisasjonen over tid, og har utviklet en del spesialtilpassede scenarier for organisasjonen.

Da denne organisasjonen jobber med finansiell risiko fra før, har organisasjonen utviklet sin egen målestokk som de ønsket at vi skulle benytte oss av. Dette er både en kvantitativ og kvalitativ målestokk. De hadde matriser tilsvarende tabell 4.4 og 4.5 for finansiell-, operasjonell- og omdømmerisiko. Konsekvensdelen var selvfølgelig litt forskjellig på hver da beskrivelsesdelen definerte kvantifiserbare hendelser. Jeg har også puttet inn arbitrære tall for å unngå å avsløre noe om bedriftens kostnadsvurderinger.

Tabell 4.4: Sannsynlighet

Navn	**Lav**	**Middels**	**Høy**	**Beskrivelse**
Veldig lav	*0%*	*10%*	*20%*	Sjeldnere enn hvert 5 år
Lav	*20%*	*30%*	*40%*	Mellom hvert 5. og 2. år
Middels	*40%*	*50%*	*60%*	Mellom hvert 2. og 1. år
Høy	*60%*	*70%*	*80%*	Mellom 1 og 2 ganger i året
Veldig Høy	*80%*	*90%*	*100%*	oftere enn 2 ganger i året

Tabell 4.5: Konsekvens

Navn	**Lav**	**Middels**	**Høy**	**Beskrivelse**
Veldig lav	*0*	*250'*	*500'*	0 til 500' i potensielle tap
Lav	*500'*	*2.500'*	*5.000'*	500' til 5.000' i potensielle tap
Middels	*5.000'*	*7.500'*	*10.000'*	5.000' til 10.000' i potensielle tap
Høy	*10.000'*	*20.000'*	*30.000'*	10.000' til 30.000' i potensielle tap
Veldig Høy	*30.000'*	*50.000'*	*70.000'*	Over 30.000' i potensielle tap

Bedriften hadde utviklet matrisene over, og det kan bare spekuleres i hvorvidt de benyttet seg av de kursiverte delene av matrisen (kursiv er fremhevet av meg). For mnemonic forholdt konsulenten seg kun til å stadfeste innenfor *beskrivelsesdelen* av den illustrerte matrisen.

Hvorvidt bedriften lærer noe eller blir mer moden enn de var fra før er ikke godt å si. Her snakker vi om en bedrift som ser på og håndterer risiko hver eneste dag. De har en innarbeidet rutine på at alle nyanskaffelser skal vurderes og analyseres først, og tankegangen er godt forankret i organisasjonens ledelse. Vi ser også at de fokuserer mye på metrikker

som kan kvantifiseres, og har utviklet egne prosentintervaller for kriteriene sine. Dette kan ha innvirkning på rapportens oppfattede legitimitet, da det til syvende og sist er en kvalifisert vurdering av analytikeren som ligger til grunn for klassifiseringen, og ikke ufravikelige forskningsresultat som danner grunnlaget for graden av risiko.

På den andre siden har flere av tjenesteleverandørene indikert at de har fått opp øynene etter en risikoanalyse, og at de har fått belyst hvor de har manglende sikkerhet. Nå er det også grunnleggende forskjeller fra den ene til den andre leverandøren, så man kan ikke hevde at alle eller ingen tjenesteleverandører har godt av risikoanalysen. Derimot kan analysen fungere som en vekker for de organisasjonene som har fokusert lite på sikkerhet og mye på funksjonalitet.

Det viktigste er uansett at rapporten sier noe om hva organisasjonen må gjøre;

- Gå videre,
- kreve implementering av virkemidler, eller i ytterste konsekvens;
- avbryte/unngå leverandøren.

En av de største utfordringene når man går igjennom en leverandør eller organisasjon etter sårbarheter, er å få tak i de rette personene, og det har forekommet at man må endre tidspunkt på avtaler fordi personer uten den etterspurte kompetansen har blitt sendt istedet for de etterspurte intervjukandidatene. Det er også en utfordring å få tak i riktig og utfyllende informasjon på forhånd slik at man heller kan benytte intervjuperioden til å grave de rette stedene.

Konsulentene har tatt med seg at det er viktig å kjenne organisasjonen godt før man gjør en risikoanalyse, da det gjerne er underliggende informasjon som ikke blir formidlet til utenforstående uten videre. Dette er erfaringer man tilegner seg, og rett bakgrunnskunnskap kan sikre bedre kvalitet i analysen.

Heller ikke i denne casen er analysen utelukkende basert på ISO 27005, men standarden har vært et essensielt verktøy i prosessen med å avdekke sårbarheter, både i konsekvensanalysen og en sårbarhetsvurdering av tjenesteleverandører.

4.3 Privat bedrift

Den siste casen er en risikoanalyse utført hos en privat nisjebedrift. De har en del lover og regler som regulerer virksomhetens aktiviteter, og trenger følgelig å være i samsvar med det som til enhver tid er gjeldende rett. Forutsetningene her var at bedriften kun ønsker å levere et produkt i et nisjemarked, og de har i utgangspunktet ikke noe forhold til risiko og -vurderinger hva gjelder informasjonssikkerhet. mnemonic hadde i forkant av denne risikoanalysen nettopp hjulpet til med å utvikle en policy for organisasjonen.

Mandatet for denne risikoanalysen var å få en oversikt over de risikoer kunden stod ovenfor, og beslutningen om å utføre en RoS-analyse var tatt av ledergruppen som en logisk forlenging av policy-arbeidet som var gjort i forkant. Organisasjonen eide beslutningen om å få analysen utført, men hadde ikke noen klare mål utover å "*avdekke risiko*". mnemonics oppgave ble derfor å vurdere prosess- og kontornettet, samt informasjonsflyten til denne kunden. Kunden forpliktet seg til å stille med de rette ressursene til rett tid. Det ble fastsatt et risikoakseptansenivå før gjennomføringen av analysen.

I likhet med de to foregående casene var fremgangsmåten noe av det samme; innhenting av informasjon ved hjelp av dokumentanalyse, workshops og intervjuer. Senere ble funnene analysert og presentert til ledergruppen. Til workshop og intervju ble kandidatene plukket ut av administrerende direktør og avdelingsledere i fellesskap, og de rollene som ble intervjuet var:

- Toppledelsen
- Avdelingsledere

- IT-avdelingen
- Systemansvarlige

Grunnen til at disse rollene ble intervjuet, var for å få kartlagt forretningsrisikoene til organisasjonen og dens avdelinger fra ledelsens side, samt å få kartlagt arkitektur og funksjonalitet hos IT-avdelingen og de systemansvarlige. På grunn av at organisasjonen var såpass liten, var det lett å få tak i rett person til rett tid. Det var et klart definert ansvarsområde på forhånd.

De ansatte ble stilt åpne spørsmål under intervjuene og på workshopen, og alle fikk anledning til å gå igjennom sine egne prosesser på en utfyllende måte. I intervjurundene ble det som regel utført intervjuer parvis eller i gruppe, og dersom man måtte ha tak i personer fra andre lokasjoner ble det foretatt telefonintervjuer.

Det ble ikke benyttet rammeverk for trusselagenter og scenarier hos denne organisasjonen. Alt ble definert på egenhånd av konsulentene basert på funn underveis i den iterative prosessen de var inne i. Man kan ikke avdekke alt, men det groveste ble avdekket og mer spesifikke scenarier kom til underveis som et supplement. Kunden hadde også mulighet til å komme med innspill dersom de følte det fantes scenarier som ikke ble dekket.

4.3.1 Funn fra case 3

Igjen ønsker jeg å avdekke organisasjonens ***motivasjon***, ***modenhet*** og ***dedikasjon***. Ved hjelp av diskusjoner og intervju med de ansvarlige konsulentene, samt et møte med en av konsulentene og IT-ansvarlig hos organisasjonen, har jeg fått et innblikk i organisasjonens prosess med sikkerhetsrisikohåndtering.

Det kan her slås fast at organisasjonen var – på tidspunktet denne analysen ble gjennomført – i den spede begynnelsen hva gjelder risikoarbeid. Det manglet ikke på dedikasjon og vilje, hverken hos de ansatte eller ledelsen, men de hadde liten kunnskap om feltet. Alle så et behov for å håndtere risiko på en skikkelig måte, da de ikke kom seg unna et høyt nivå av risiko ved

enkelte aspekter av forretningen sin. Videre var også intensjonen for å utføre risikoanalysen god, selv om den var litt uspesifisert. Det ble for eksempel observert at akseptansenivåene som ble satt i forkant av analysen, viste seg å bomme på intensjonen organisasjonen egentlig hadde.

Det var heldigvis definert på forhånd hvem som hadde ansvar for hvilke aspekter ved forretningsprosessene, noe som ga grunnlag for å ta tak i eventuelle funn hos organisasjonen.

De ansatte hadde generelt god kunnskap hva angikk deres eget fagområde, men da det kom til sikkerhet var dette noe de var nysgjerrige på uten å inneha noe spesiell kunnskap om. Dette er et godt utgangspunkt for videre arbeid med **awareness**, men det betyr også at organisasjonen ikke var modne nok i alle ledd til å bedrive risikoanalyser.

Konsulentene definerte en målestokk lik tabellene 4.1, 4.2 og 4.3. I tillegg ble det benyttet en matrise tilsvarende tabell 4.6. Dette var basert på bransjestandarder, konsulentens egne erfaringer og i samråd med bedriftens ledelse. Konsulenten hadde en praktisk-pragmatisk tilnærming til målestokkene, og ønsket å tilpasse den til organisasjonens behov.

Tabell 4.6: Konsekvensskala

Konsekvens	Økonomi	Liv og Helse	Omdømme	Lovregulering	Tilgjengelighet
Høy	Finansielle tap over 100mill	Det oppstår kritiske personskader, inkludert tap av liv eller livstruende skader	Det oppstår store skader på organisasjonens anseelse, dvs skade som ikke kan gjenopprettes	Alvorlige lovbrudd som fører til fengsels- eller virksomhets-straff (miste retten til å drive virksomhet)	Kritiske systemer utilgjengelige > 24 timer
Middels	Finansielle tap mellom 10mill og 100mill	Det oppstår betydelige personskader men som ikke omfatter tap av liv eller livstruende skader	Det oppstår betydelige skader på organisasjonens anseelse som tar mer enn 1 år å gjenopprette	Mindre alvorlige lovbrudd som fører til bøter	Kritiske systemer utilgjengelige < 3 timer men > 24 timer
Lav	Finansielle tap inntil 10mill	Det oppstår mindre personskader	Det oppstår mindre skader skader på organisasjonens anseelse som tar mindre enn 1 år å gjenopprette	Mindre alvorlige lovbrudd eller forseelser som fører til advarsel eller pålegg	Kritiske systemer utilgjengelige < 3 timer

Det var kombinasjonen av de forhåndsdefinerte akseptansenivåene og konsekvensskalaen som førte til at organisasjonens eneste valg var å stanse all aktivitet for å unngå uakseptabel risiko. Dette fikk de reagert på, og omdefinerte både risikoakseptansenivået og scenariet slik at resultatet ble nyttigere. Man kan derfor si at man, både konsulenter og organisasjonen selv, lærte mer av selve risikoanalysen enn selve resultatet av denne. De ansatte har blitt mer bevisste, de forskjellige avdelingene har sett at IT-risiko henger sammen med forretningsrisiko og ledelsen vet nå hva de vil med fremtidige

risikoanalyser. De har innsett at det er viktig med et forhold til risiko på et due diligence-nivå for å drive forsvarlig, og at iterativt risikoarbeid sørger for at de ansatte er bevisste på sitt forhold til informasjonsrisiko.

Del III

Diskusjon, konklusjon og anbefalinger

KAPITTEL 5

Diskusjon og konklusjon

I de to foregående kapitlene, 3 og 4, har jeg sett på ISO 27000-serien, alternativene, og forskjellige forståelser av *risiko*. Jeg vil i dette kapittelet diskutere mine tre hovedspørsmål, definert i 1.2.1, før jeg foreslår en mulig løsning. Da det er store sammenhenger mellom to av spørsmålene mine, slår jeg disse sammen i en del. Kapittelet blir derfor delt i fire deler, to til problemstillingene mine, en del viet til introduksjon av **risikoobjekter**, og en til avsluttende konklusjon.

5.1 Hvordan påvirkes risikoarbeid i en organisasjon av risikoforståelsen, og hva er forutsetningen for et vellykket risikoarbeid?

Som vi kan se i den nevnte litteraturen, er det store forskjeller på hvordan man definerer risiko. Det er også delte meninger om hva risiko innebærer, og med et så fragmentert fagfelt, er det vanskelig å enes om en standardisert

fremgangsmåte for risikovurderinger. Jeg ønsker derfor å først ta tak i definisjonene av risiko. Av de tidligere nevnte definisjonene, kan vi dele dem inn i fire kategorier. Den første er de som mener at risiko kun er sannsynligheten for en uønsket hendelse eller utfall. Dette mener Graham & Wiener [25], og Cambell [10]. Den andre hovedkategorien er de som mener at risiko er et produkt av sannsynlighet og konsekvens. ISO [31], Kaplan & Garrick [35], Kaplan [34] og Lowrance [38] havner i denne gruppen. Det interessante her, er at ISO har sluttet seg til denne definisjonen av risiko. Dette kommer jeg til å ta fatt i senere. Den tredje, som også er den største gruppen av definisjoner, er de som mener at risiko er et uvisst utfall av en situasjon, der **noe** som **noen** verdsetter er utsatt. Blant annet mener Aven & Renn [6], Renn [46], Rosa [48, 49] og Wikipedia [54] at dette er den optimale definisjonen av risiko. I den fjerde og siste gruppen finner vi definisjonen av risiko i følge Google [22]. Denne definerer risiko som en situasjon som involverer utsettelse for fare, uten å ta stilling til om det er en selv eller noe man verdsetter som utsettes for denne faren. Dette samsvarer med den italienske betydningen av *risicare* [7].

Fellesnevneren for alle definisjonene, med unntak av definisjonen til Kaplan [34] og Kaplan & Garrick [35], er at risiko blir sett på som noe negativt. Man må gjøre seg opp en formening om gevinsten i andre enden kan overskygge risikoen man må utsettes for underveis. De norske og internasjonale standardene NS5830-prNS5832 [40, 41, 42] og ISO 27000-serien [27, 31] ønsker å ta vurderingen av gevinst/positiv konsekvens av unngåelse av en negativ hendelse, ut av risikoanalysen, og lar dette være en aktivitet utenfor standardens virkeområde. Det forutsettes derimot i ISO 27005 [31] at dette er utført, da de forventer et risikoakseptansenivå som input til risikovurderingsaktiviteten. Dette kan man kun spekulere i om er fordi man forutsetter at aktivitetens gevinstgrad er grunnleggende høy hvis man ønsker å vurdere risiko i aktiviteten.

I de tre casene jeg har sett på i kapittel 4, er det også en forutsetning

at den innleide konsulenten ikke tar hensyn til de positive konsekvensene. I alle casene har konsulentens oppgave vært å avdekke risiko i forståelsen; sannsynlighet for at noe negativt skal inntreffe, og potensielle konsekvenser ved de negative hendelsene. Videre har alle de nevnte organisasjonene latt det være opp til konsulenten å definere risikoscenariene. I tilfellene hos finansinstitusjonen (kapittel 4.2) og den offentlige organisasjonen (kapittel 4.1), har konsulenten hovedsakelig støttet seg på SANS [26] og deres kritiske virkemidler og scenarier. Hos den private bedriften i 4.3 ble det laget scenarier i samråd med kunden. Videre er det innad i mnemonic supplert med ytterlige scenarier som er ofte observert fra deres trusseletterretningsarbeid. I tråd med ISO 27005 [31], har mnemonic funnet en måte å gjøre aktivitetene som foreslås. Ved å forstå risiko på en måte som er hovedsakelig fakta-orientert og pragmatisk, har de utviklet en metode som først avdekker mulige konsekvenser. Dette gjør det mulig å identifisere kritiske systemer og forretningsrisikoer, og informasjonen benyttes i det videre arbeidet. Det videre arbeidet består i å identifisere måter forretningsrisikoene kan inntreffe. Når man kjenner til potensielle scenarier skal det avdekkes i hvilken grad det finnes muligheter for at scenariene er gjennomførbare. Dette gjør de ved at de støtter seg på Intels Threat Agent Library [50], teknisk kompetanse, penetrasjonstester og intervjuer.

Hos de kundene med en grunnleggende forståelse for risiko, slik som i 4.2, vil dette produsere et resultat kunden kan ta tak i. Hos kunder som kun utfører risikovurderinger for å oppnå et revisorstempel, vil ikke resultatet av risikovurderingen være like nyttig.

Jeg snakket i kapittel 4 om *motivasjonen*, *modenheten* og *dedikasjonen* til kunden. De generelle funnene jeg observerte, var at dedikasjonen og motivasjonen hang sammen med risiko*forståelsen*. Modenheten indikerte gjerne hvor lenge motivasjonen hadde vært høy, og hadde i så måte ikke noen individuell, direkte innvirkning på kvaliteten på risikoarbeidet. Dette støttes av funnene fra 4.3. Her hadde man en bedrift som hadde identifisert et behov for

formelt risikoarbeid, men ingen reell erfaring. Motivasjonen og dedikasjonen var generelt høy, mens modenheten var lav. Her fikk konsulenten utføre en risikovurdering på sine egne premisser, mens kunden ville være med på å definere scenariene. Dette førte til at risikoscenariene ble uhensiktsmessig formulert. Dette kan illustreres med et parallelt eksempel fra et lignende forretningsområde. Kunden kunne ikke akseptere risiko for liv og helse, og skisserte et scenario der hvor ansatte utsatte seg selv for livsfare. En tenkt parallell her, er en elektrikerbedrift. Hvis man ikke er forsiktig kan de ansatte faktisk dø av elektrisk sjokk. Da bedriftens forretningsområde innebar fare for liv og helse til enhver tid, opplevde de at de risikovurderingen tilsa at de måtte slutte med sine tjenester. Dette er mot sin hensikt, da bedriften innså at de ikke kunne slutte med oppgavene sine, man måtte heller implementere virkemidler som reduserte risikoen til et akseptabelt nivå.

Hos den offentlige organisasjonen 4.1, var både motivasjonen og modenheten lav. Dedikasjonen, på den andre siden, var høyere. Her hadde det kommet en lov som tilsa at alle offentlige organisasjoner innenfor sektoren måtte "*utføre regelmessige risikovurderinger*". For å være i samsvar med loven ønsket organisasjonen å utføre risikovurderinger annet hvert år. Her hadde konsulenten vært innom to år tidligere og utført en tilsvarende risikoanalyse, så både konsulent og organisasjon hadde praktisert øvelsen tidligere. Det var derfor å forvente at organisasjonen hadde håndtert risikoene som ble påpekt tidligere. Dette var i stor grad ikke tilfelle, og mange av de tidligere sårbarhetene og ikke-akseptable risikoene var ikke gjort noe med. Dette kan indikere at organisasjonen ikke har en god forståelse for hva risiko er, og hvorfor det er viktig at risiko håndteres og overvåkes kontinuerlig.

I alle tilfellene var det gitt et tilbud på risikovurdering, og alle tilbudene inneholdt en tidsramme. Det var derfor en forutsetning at risikovurderingen ikke ville gå ut over den avtalte tiden, og det var en underforstått enighet om at man skulle presentere et resultat som traff innenfor et forhåndsdefinert virkeområde. I forbindelse med spørsmålet om forbrukt tid vil ha innvirkning på

resultatet, kan vi se av 4.3 at dette var tilfellet. Her hadde bedriften en bratt læringskurve, og mer forbrukt tid ville gitt en bedre forståelse. På den andre siden ville en økning i forbrukt tid hos 4.1 ikke ført til en økning i kvaliteten på resultatet av risikovurderingen. I det siste tilfellet 4.2, har de et sunt forhold til risikoarbeid, og utfører kontinuerlig risikoarbeid. Her var oppgaven å avklare spesifikke risikoer, og det ble satt av tilstrekkelig med tid for å få et så grundig resultat som organisasjonen ønsket.

Å være konsulent innen risiko kan derfor sammenlignes med å være en stjernekokk. Hvis den som bestiller dine tjenester ikke forstår hva man bestiller, vil man kanskje ende opp med å bestille noe helt annet enn det man har lyst på og behov for.

Her er det derfor viktig at man forholder seg til en standard som er både god og universell. Dette gjør det lett for folk å forstå de forskjellige prosessene og ansvarsområdene i risikoarbeid. En konsulent har et enormt ansvar for å sørge for at selv kundene med liten forståelse for risiko får et godt resultat. I mnemonic er konsulentene sitt ansvar bevisste, og setter sammen aktivitetene på en måte som også øker forståelsen og bevisstheten hos de kundene som ikke har god kjennskap fra før. Derfor er det viktig for en konsulent å ha gode, forhåndsdefinerte rammeverk som man kan hente ut aktiviteter fra.

5.2 Hvordan kan aktivitetene og resultatene i ISO 27005 formaliseres?

Da oppgaven omhandler ISO 27005, ønsker jeg å sette denne sentralt i diskusjonen. Jeg skal belyse de problematiske aspektene som reiser seg rundt håndtering av risiko ved å følge standarden. Først ønsker jeg å se konseptene i standarden opp mot begrepet risiko. Som nevnt tidligere skal man i følge standarden først etablere kontekst, deretter skal man *vurdere, behandle, akseptere, kommunisere, gjennomgå* og *overvåke* risiko. Det står ikke noe

om hvordan man skal definere risiko ut over "*et produkt av sannsynlighet og konsekvens*", og som nevnt i de foregående kapitlene, kan man definere risiko på mange forskjellige andre gyldige måter.

Som nevnt tidligere, ønsker ISO 27005 [31] at man regner ut risiko. I det følgende forutsettes det at risiko anses som noe negativt. På denne måten blir det enklere å kalkulere konsekvens, da man ikke trenger å ta høyde for gevinsten ved unngåelse av en negativ hendelse. Videre foreslår standarden at man setter verdier på både sannsynligheten og konsekvensen ved at man gjør en "*vurdering*". Hva denne vurderingen går ut på er dårlig forklart i selve standarden, og kan for mange fremstå som svart magi. "*Garbage in, garbage out*" (GIGO), som er et begrep innen informatikk, går ut på at en datamaskin kan gjøre det den er programmert til med input, og følgelig også produsere en outputverdi. Dersom du kjenner input og forstår hva programmet gjør, har dette en utmerket hensikt, men hvis input er meningsløse data, kan det ikke forventes at programmet produserer et fornuftig resultat. Et annet aspekt ved GIGO er at man i alt for stor grad lar det være opp til en datamaskin hva man skal foreta seg. Man antar at verdien man får ut av programvare man kjøper alltid er nyttig og korrekt, noe som ikke alltid har vist seg å stemme.

Det er også her jeg stiller spørsmålstegn ved fremgangsmåten foreslått av ISO 27005. Etter å ha delt inn konsekvensene i nivåer, behandles sannsynlighet. ISO 27005 [31] nevner at sårbarheter, scenarier, trusler og aktiva har en innvirkning på sannsynlighet. Men som vi har observert i 5.1 kan resultatene bli meget varierende uten en bedre spesifikasjon på hvordan dette henger sammen, og hvordan man best kan avdekke denne informasjonen. Da det er forskjeller på folks risikoaversjon og -appetitt [7, 32, 33] avhengig av forskjellige situasjoner og forutsetninger, kan man ende opp med forskjellige sannsynlighetsverdier avhengig av konsulentens dagsform. Det er derfor viktig at man formaliserer forståelsen av risiko i større grad. Det er når man overlater definisjonen til tolkning at dårlig forståelse kan føre til dårlige resultater.

5.3 Risikoobjekter

Som vi har sett hittil i oppgaven, samsvarer de forskjellige standardene ganske godt med hverandre. Det er lite som skiller dem fra hverandre på det konseptuelle planet, det er tilnærmingen som er forskjellig. Den mest vesentlige forskjellen i den belyste litteraturen, er hvordan de mener at risiko skal forstås og defineres. Fellesnevneren for risikodefinisjonene derimot, er at de omtaler risiko som noe negativt. Enten er det den negative konsekvensen av en hendelse som påvirker noe man vil passe på, kombinert med sannsynligheten for at den nevnte hendelsen vil inntreffe, eller så er det en hendelse som vil påvirke noe med usikkert utfall.

Jeg synes tankegangen her er god, og ønsker å legge til grunn at det abstrakte begrepet risiko omhandler noe negativt. Derimot ønsker jeg å utfordre dagens generelle forståelse av risiko. Resten av informatikken har formelt forholdt seg til objekter siden 1960-tallet, da Ole-Johan Dahl og Kristen Nygaard introduserte SIMULA. Hvorfor må risiko være et produkt, eller en sum av noe? Hvorfor kan det ikke behandles som et objekt?

Risiko er tydeligvis så vanskelig å definere, at vi lett kan finne ti forskjellige definisjoner. Alle er like gode, og man ser hensikten og poenget med alle sammen. De sier forskjellige ting, men betyr i praksis det samme. Samtidig har Terje Aven ledet oss igjennom et antall oppfatninger av risiko som har fotfeste, men som han allikevel prøver å motbevise. Dette tilsier bare at risiko er individuelt og subjektivt. Kan vi ikke da prøve å samle de objektive faktorene bak risiko? Hver eneste faktor vi kan påpeke vil bli sett på som et attributt i den store risikosekken.

Gjennom arbeidet i mnemonic, og med samtaler med flere av de ansatte, har det blitt tydelig at ISO 27005 kun er noe man har i bakhodet mens man utfører punktene i ISO 27001 og ISO 27002. Det har vært diskutert i hvilken grad man ser på ISO 27005 som nyttig eller overflødig, men resultatet har i alle diskusjoner vært at man kan falle tilbake på enkelte attributter for

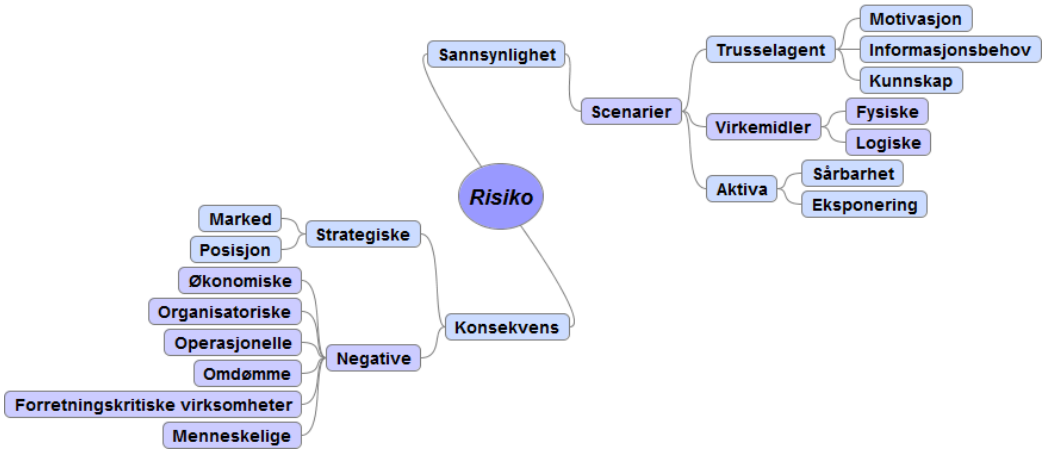
å måle risiko, og at standarden med vedlegg har vært med på å utvikle mnemonics fremgangsmåte. Da mnemonic også har forskjellige kunder i forskjellige bransjer, har det også blitt erfart at en pragmatisk objekt-tilnærming av risiko vil gi matnyttige resultater uansett hva slags organisasjon som må forholde seg til risiko. Siden man ikke kan garantere fremtiden, er det vesentlig å avdekke potensielle utfall, og med en objektforståelse av risiko vil man kunne ha en tilnærming der man avdekker de mest kritiske utfallene.

At både NIST [43, 45, 44] og ISO [27, 28, 29, 31, 16, 17] har utviklet standarder for hvordan man skal håndtere risiko samtidig som Standard Norge også holder på å utvikle en rekke forslag [40, 41, 42] for å formalisere fremgangsmåten i en risikovurdering, illustrerer dette kun behovet for å endre definisjonen av risiko.

La meg så få presentere de grunnleggende attributtene i risikoobjektet. Som to hovedattributter har vi **sannsynlighet** og **konsekvens**. Det er foreløpig ikke noe banebrytende her, da sannsynlighet og konsekvens har blitt omtalt i flere av definisjonene fra kapittel 3.3. Jeg ønsker derimot her å også samle de følgende attributtene i begrepet **scenario**: **trusselagent** – med **kunnskap**, **motivasjon**, og **informasjonsbehov**; **virkemidler** – med **fysiske** og **logiske**; **aktiva** – med **eksponering** og **sårbarheter**. Disse utgjør det man klassisk anser å utgjøre **sannsynlighet**. På den andre siden av risikoobjektet ønsker jeg å samle **konsekvensene**: de **negative** konsekvensene innehar; **organisatoriske** konsekvenser, **økonomiske** konsekvenser, **operasjonelle** konsekvenser, **omdømme**konsekvenser, **forretningskritiske** konsekvenser og **menneskelige** konsekvenser. De **strategiske** konsekvensene innehar **markeds**konsekvenser og **posisjons**konsekvenser. En del av disse attributtene høres kanskje rare ut, og vil kanskje ikke gi noen mening tatt ut av sammenhengen. Jeg ønsker derfor å referere til figurene 5.1 og 5.2. I figur 5.1 vil jeg illustrere en kjent tegning med sannsynlighet og konsekvens. I 5.2 vil jeg plassere attributtene på en slik måte at sammenhengen blir opplagt og logisk. Det vil også være mulig å kunne gå igjennom attributtene en etter en, forbundet

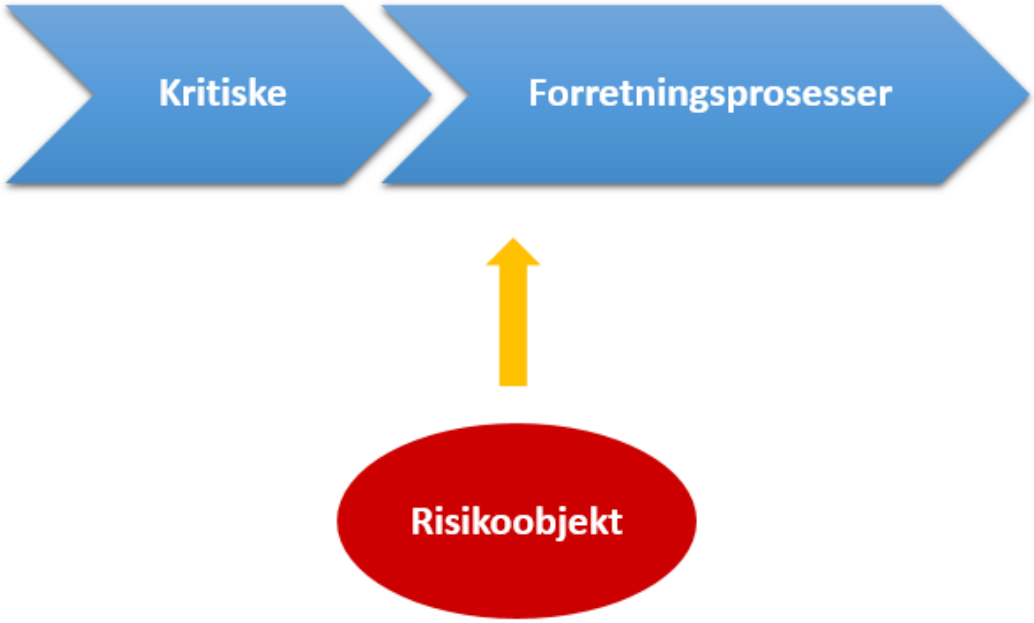
med forskjellige forretningsrisikoer, og sammen vil alle attributtene utgjøre det individuelle risikoobjektet. Objektet må sees i sin helhet, der attributtene samles fra kantene og inn til midten.

Figur 5.1: Forståelse av et generisk risikoobjekt.



Figur 5.2: Utvidet forståelse av et generisk risikoobjekt.

I likhet med standarden, har jeg unnlatt å snakke om begrepene *gevinst* og *positiv konsekvens*. Dette fordi jeg mener vi må anse gevinst og positive konsekvenser som en del av de kritiske forretningsprosessene. Risikoobjektet vil ha en innvirkning på de forretningskritiske prosessene, så det er viktig at disse prosessene avdekkes samtidig som konsekvensene avdekkes. Da får man også gjort seg opp en formening om hvilket akseptansenivå man skal legge seg på. Se figur 5.3 for illustrasjon av hvordan et risikoobjekt har innvirkning på forretningsprosessene.



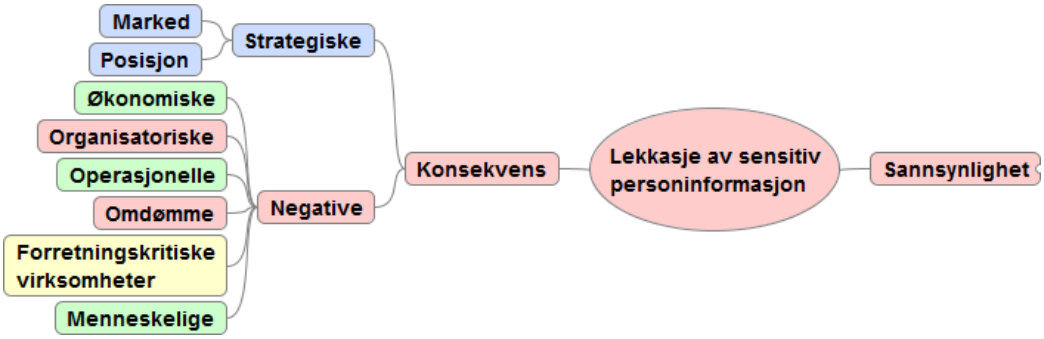
Figur 5.3: Hvordan risiko har innvirkning på forretningsprosesser.

Som vi kan se av figur 5.2, er det her mulig å gå igjennom de forskjellige risikoene man står overfor, og plotte inn fakta i de respektive attributtene. Jeg ønsker å illustrere dette med et tenkt scenario, der man står overfor risikoen *datalekkasje*, se figur 5.4.

Figur 5.4: Konsekvens og sannsynlighetsattributtene til risikoobjektet “datalekkasje”.

Jeg har i figur 5.5 valgt å fargelegge attributtene, for å indikere mine eksempelverdier. Jeg har valgt å holde meg til en kvalitativ skala med tre trinn; lav, middels og høy. Fargen grønn representerer lav, gul representerer

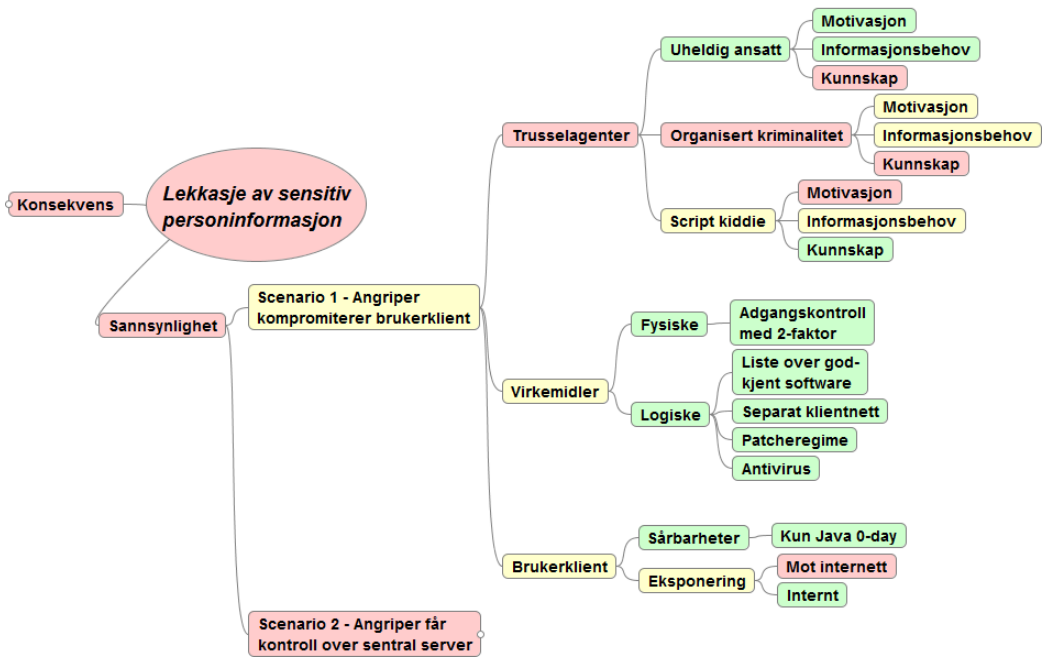
middels, og rød representerer høy. Dette er normalt verdier som vil avdekkes under vurderingsfasen av risiko, som nevnt i ISO 27005.



Figur 5.5: Konsekvensdelen av datalekkasje-risikoobjektet.

I figur 5.5 har jeg valgt å vise hvordan et tenkt resultat av en konsekvensanalyse for forretningsrisikoen “lekkasje av sensitiv personinformasjon”. I dette eksemplet (5.5), vil vi se at det ikke er noen strategiske konsekvenser. De negative konsekvensene blir vurdert til å være høye, da omdømmet er viktig for de fleste organisasjoner. Her er det gravd i organisasjonen, og avdekket hvordan de ser for seg konsekvensene uten noen særlige virkemidler implementert.

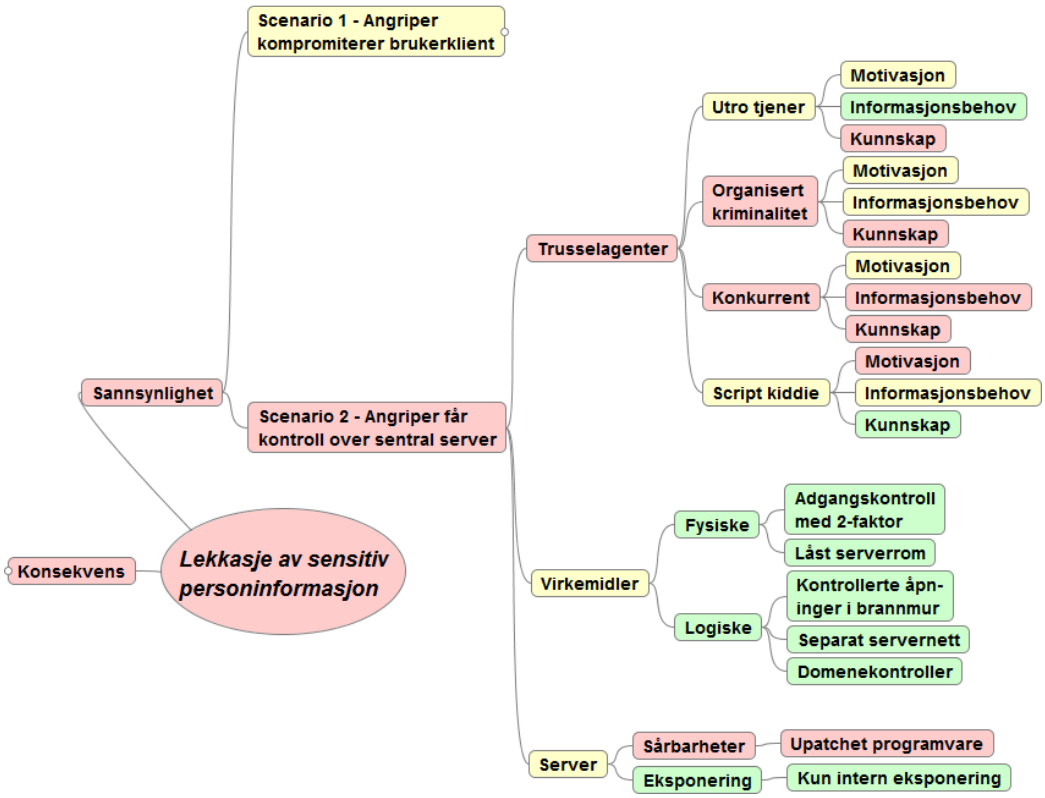
Hvis vi tar en titt på 5.6 og 5.7, så har jeg prøvd å kartlegge de andre attributtene. Dette kan man best gjøre ved å definere scenarier. I tillegg til å ha en liste over de 20 mest kritiske virkemidlene, har SANS [26] også laget en liste over de vanligste angrepsscenariene. Disse er basert på empiri fra hele verden, og i den grad noen kan hevde at de har et statistisk signifikant referanseutvalg, så må det være dem. Her er det også hentet inn kunnskaper om trusselagentene, basert på den beste tilgjengelige erfaringen. Intel [50]



Figur 5.6: Scenario 1-delen av datalekkasje-risikoobjektet.

har laget et bibliotek over de vanligste trusselagentene, og beskrevet deres *modus operandi*. Kombinerer man tiltakslisten i ISO 27002 [29], SANS Top 20 virkemidler [26] og andre godt dokumenterte virkemiddelslister [2], kan man uttale seg om hvilke virkemidler organisasjonen har på plass, eventuelt hvilke de mangler. Jeg har valgt å kun ta med de som er implementert i den fiktive bedriften, for å illustrere hvordan dette kan fungere. Illustrasjonen vil bli alt for omfattende dersom det skal utføres en fullstendig – fiktiv – vurdering.

I dette eksemplet har vi skissert to forskjellige angrepsscenarier, der en angriper enten kompromitterer en brukerklient eller får urettmessig tilgang til en tjener. Jeg har derfor valgt å illustrere aktiva med hhv. “brukerklient” og “server” i de to scenariene. Sårbarheter avdekkes best ved en grundig teknisk penetrasjonstest eller gode dybdeintervjuer med de teknisk ansvarlige for løsningen. Der dette ikke er mulig må man støtte seg på *threath intelligence*-kilder. Disse finnes det blant annet mange av fritt tilgjengelige på internett. Det viktigste når man skal avdekke sårbarheter er at man avdekker så mye

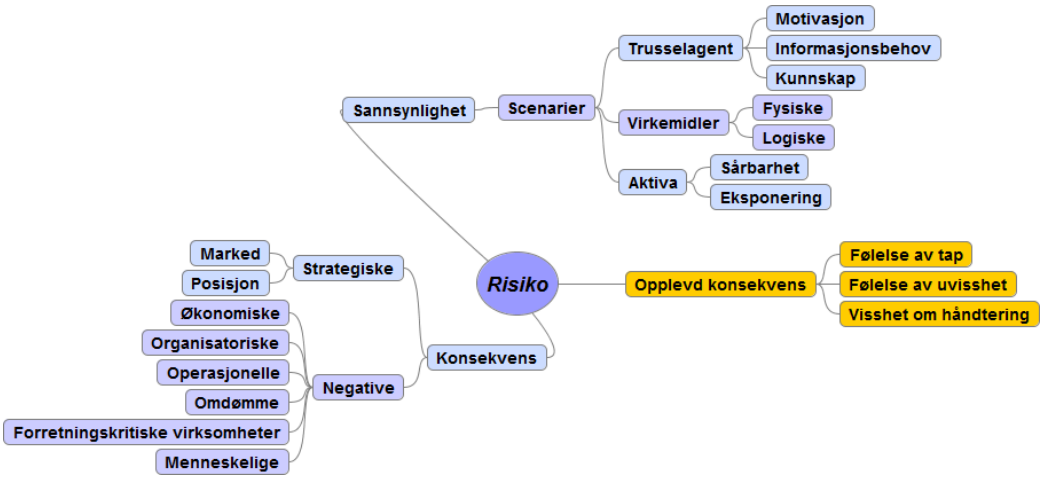


Figur 5.7: Scenario 2-delen av datalekkasje-risikoobjektet.

informasjon som mulig, og at man forholder seg faktaorientert og analytisk til materialet.

Med en objektorientert forståelse av risiko tar man også høyde for at risikoaversjon eller -appetitt avhenger av i hvilken grad personen er trygg på utfallet [7, 32, 33]. Jo mer informasjon man har avdekket i en modell tilsvarende 5.2, jo tryggere er man på at man har dekket alle utfallene, og man kan ta en analytisk avgjørelse av hvorvidt forretningsrisikoen er en akseptabel risiko eller ikke.

Målet med en risikovurdering må være å redusere den ubegrunnede, subjektive følelsen av at noe er eller kommer til å gå galt. For å illustrere dette har jeg laget en tredje arm på risikoobjektet 5.8. Denne armen vil alltid være til stede, nettopp slik som Bernoulli [7], Kahneman [33] og Jøsang & Lo Presti



Figur 5.8: Den irrasjonelle følelsesdelen av datalekkasje-risikoobjektet.

[32] påpeker – poenget må være å redusere hvor mye man vektlegger denne armen istedet for de to andre.

En annen faktor, som også spiller inn, er i hvilken grad man er viss på at man kan takle konsekvensene av en uønsket hendelse. Eksempler på dette er scenarier med omdømmetap som konsekvens. Hvis man er flink på å håndtere relasjonen til omverdenen i etterkant av en slik hendelse, så kan man redusere konsekvensen i etterkant. Blant annet skjer det hendelser i den politiske sfære hvor man takket være god håndtering får redusert den inntrufne hendelsens innvirkning på omdømmet. Dette er en vurdering man selv gjør basert på erfaring fra tidligere håndterte hendelser, og kan heller ikke garanteres, derfor er den plassert på jokerarmen til risikoobjektet.

5.4 Konklusjon og anbefalinger

Jeg har i min oppgave ønsket å se på hvordan risiko bør forstås. Jeg har også ønsket å se på hva som er forutsetningene for et vellykket risikoarbeid, og hvordan risikoforståelsen kan påvirke risikoarbeidet i en organisasjon. Jeg har derfor sett på hvordan risiko blir definert, og hvordan det blir håndtert i en rekke organisasjoner. Dette har jeg så sett opp mot gjeldende standarder fra NIST,

ISO og Standard Norge, med særlig vekt på ISO 27005 [31].

Som en konklusjon på oppgaven min, ønsker jeg å påpeke noen momenter. Det er ingen store konseptuelle forskjeller på de relevante eksisterende standardene. Alle ønsker at man i forbindelse med risikoarbeid avdekker sårbarheter, konsekvenser, aktiva og sannsynlighet. Der jeg mener at ingen av standardene har klart å kommunisere det viktige faktum at risiko **ikke** er lineært innen informasjonssikkerhet. Det går ikke an å regne ut sannsynligheten for at et scenario inntreffer, for det er så mange ting som kan spille inn. For de fleste organisasjonene er det snakk om at man har et coprodukt, altså at enten det ene *eller* det andre scenariet kan inntreffe. I en risikoanalyse er det i praksis aldri mulig å lage en uttømmende liste over scenarier som truer bedriftens forretningsrisikoer, men man kan ta for seg de mest kritiske scenariene. Her kan man finne sårbarheter, potensielle trusselagenter og implementerte virkemidler, og jo flere av scenariene man går igjennom, jo flere måter avdekker man at en potensiell angriper kan komme seg til kjerneinformasjonen som man ønsker å beskytte. Det er et gammelt ordtak som sier: "*Alle veier fører til Rom*", og derfor hjelper det ikke å sette opp bomstasjon kun på hovedveien – da tar folk heller småveiene inn.

Siden vi også har sett at godt risikoarbeid henger tett sammen med risikoforståelsen i en bedrift, så er det opp til den innleide konsulenten å forklare risiko på en måte hvor mottaker av informasjonen forstår hvorfor det er viktig å avdekke mest mulig informasjon; og at det er viktig at denne informasjonen er så riktig og nøyaktig som mulig. Det er ikke mulig å standardisere hva som er risiko, og hva som ikke er det. Det er derimot mulig å definere risiko på en slik måte at alle som skal vurdere sin egen risiko får avdekket de attributtene som er relevante for en selv. Derfor har jeg ønsket å foreslå objektorientert tenkning innen risiko. Innen informasjonssikkerhet vil det finnes enigheter om at det er visse faktorer som avgjør grad av risiko, og jeg har derfor prøvd å illustrere hvordan de henger sammen.

Bibliografi

[1] General Assembly. Report of the United Nations conference on environment and development. Technical report, United Nations, 1992. http://www.un.org/documents/ga/conf151/aconf15126-1annex1.htm.

[2] Australian Government, Department of Defence Intelligence and Security. Strategies to Mitigate Targeted Cyber Intrusions. Accessed online.

[3] Terje Aven. *Foundations of Risk Analysis*. John Wiley & Sons. Ltd, 2003.

[4] Terje Aven. *Risk Analysis - Assessing Uncertainties Beyond Expected Values and Probabilities*. John Wiley & Sons. Ltd, second edition, 2009.

[5] Terje Aven. *Misconceptions of Risk*. John Wiley & Sons. Ltd, first edition, 2010.

[6] Terje Aven and Ortwin Renn. On risk defined as an event where the outcome is uncertain. *Journal of Risk Research*, 12:1–11, 2009.

[7] Peter Lewyn Bernstein. *Against the Gods: The Remarkable Story of Risk*. John Wiley & Sons. Inc. New York, 1996.

[8] Michael H Birnbaum. *International Encyclopedia of the Social and Behavioral Sciences*, chapter Decision and Choice: Paradoxes of Choice, page 3286–3291. Elsevier, 2001.

[9] British Government. Health and Safety at Work etc. Act 1974, 1974. http://www.legislation.gov.uk/ukpga/1974/37/contents.

[10] Scott Cambell. Determining Overall Risk. *Journal of Risk and Research*, 8(7/8):569–581, 2005.

[11] Gerolamo Cardano, Jacob Bernoulli, and Simeon Dennis Poisson. Law of Large Numbers. Accessed online, wikipedia.

[12] Gibson Research Corporation. How Big is Your Haystack? ... and how well hidden is **YOUR** needle? http://www.grc.com/haystack.htm.

[13] National Vunerability Database. Number of Java vulnerabilities by year. Accessed online.

[14] Baruch Fischhoff. Risk perception and communication unplugged: twenty years of process. *Risk Analysis*, 15:137–145, 1995.

[15] Organisastion for Economic Co-Operation and Development. OECD Principles of Corporate Governance. Technical report, Organisastion for Economic Co-Operation and Development, 2004. http://www.oecd.org/corporate/ca/corporategovernanceprinciples/31557724.pdf.

[16] AS/NZS/International Organization for Standardization. AS/NZS ISO 31000:2009 - Risk Management – Principles and Guidelines. Standard, 11 2009.

[17] International Organization for Standardization. ISO Guide 73:2009 - Risk Management – Vocabulary. Standard, 2009.

[18] Standard Norge/International Organization for Standardization. NS-ISO/IEC 9001:2000 - Quality management systems – Requirements. Standard, 12 2000.

[19] Standard Norge/International Organization for Standardization. NS-ISO 14001:2004 - Environmental management systems – Requirements with guidance for use. Standard, 04 2004.

[20] Google.com. Define: assurance. Accessed online.

[21] Google.com. Define: certainty. Accessed online.

[22] Google.com. Define: risk. Accessed online.

[23] Google.com. Define: safety. Accessed online.

[24] Google.com. Define: security. Accessed online.

[25] John D. Graham and Jonathan Baert Wiener, editors. *Risk versus Risk: Tradeoffs in Protecting Health and the Environoment*. Hardvard University Press, 1995.

[26] SANS Institute. Critical Controls for Effective Cyber Defense. Technical report, SANS, 2013.

[27] ISO/IEC. NS-ISO/IEC 27000:2009 - Information Technology – Security techniques – Overview and Vocabulary. In *IT-Sikkerhet – Et utvalg av standarder i NS-ISO/IEC 27000-serien*. Standard Norge/International Organization for Standardization, 06 2012.

[28] ISO/IEC. NS-ISO/IEC 27001:2005 - Information Technology – Security techniques – Information security management systems – Requirements. In *IT-Sikkerhet – Et utvalg av standarder i NS-ISO/IEC 27000-serien*. Standard Norge/International Organization for Standardization, 06 2012.

[29] ISO/IEC. NS-ISO/IEC 27002:2005 - Information Technology – Security techniques – Code of Practice. In *IT-Sikkerhet – Et utvalg av standarder i NS-ISO/IEC 27000-serien*. Standard Norge/International Organization for Standardization, 06 2012.

[30] ISO/IEC. NS-ISO/IEC 27004:2009 - Information Technology – Security techniques – Information security management – Measurement. In *IT-Sikkerhet – Et utvalg av standarder i NS-ISO/IEC 27000-serien*. Standard Norge/International Organization for Standardization, 06 2012.

[31] ISO/IEC. NS-ISO/IEC 27005:2011 - Information Technology – Security techniques – Information security risk management. In *IT-Sikkerhet – Et utvalg av standarder i NS-ISO/IEC 27000-serien*. Standard Norge/International Organization for Standardization, 06 2012.

[32] Audun Jøsang and Stéphane Lo Presti. Analysing the Releationship Between Risk and Trust. *Second International Conference on Trust Management*, pages 135–145, 2004.

[33] Daniel Kahneman. *Thinking Fast and Slow*. Penguin Books Ltd., 2011.

[34] S. Kaplan. *Risk assessment and risk management - basic concepts and terminology*. Hemisphere, 1991.

[35] S. Kaplan and B.J. Garrick. On the quantitative definition of risk. *Risk Analysis*, 1:11–27, 1981.

[36] Frank Hyneman Knight. *Risk, Uncertainty and Profit*. Houghton Mifflin, 1921.

[37] Dennis Victor Lindley. *Understanding Uncertainty*. John Wiley & Sons. Inc., 2006.

[38] William W. Lowrance. *Of Acceptable Risk: Science and the Determination of Safety*. William Kaufmann Inc., 1976.

[39] Randall Munroe. Password Strenght. http://xkcd.com/936/.

[40] Standard Norge. NS5830:2012 - Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Terminologi. Standard, 06 2012.

[41] Standard Norge. prNS5831 - Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Risikohåndtering. Standard, 01 2013. Høringsversjon.

[42] Standard Norge. prNS5832 - Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Risikoanalyse. Standard, 01 2013. Høringsversjon.

[43] NIST (National Institute of Standards and Technology). NIST Special Publication 800-30 - Revision 1 – Guide for Conducting Risk Assessments. Standard, 11 2009.

[44] NIST (National Institute of Standards and Technology). NIST Special Publication 800-39 – Managing Information Security Risk – Organization, Mission, and Information Security View. Standard, 03 2011.

[45] NIST (National Institute of Standards and Technology). NIST Special Publication 800-37 - Revision 1 – Guide for Applying the Risk Management Framework to Federal Information Systems – A Security Life Cycle Approach. Standard, 09 2012.

[46] Ortwin Renn. Towards an integrative approach. White paper on risk governance, International Risk Governance Council, Geneva, 2005.

[47] Jacques Richardson. Weighing foresight with due diligence and the precautionary principle. *forsight*, 11(1):9–20, 2009.

[48] Eugene A. Rosa. Metatheoretical foundations for post-normal risk. *Journal of Risk Research*, 1:15–44, 1998.

[49] Eugene A. Rosa. *The Social Amplification of Risk*, chapter The logical structure of the social amplification of risk framework (SARF): metatheoretical foundation and policy implications. Cambridge University Press, 2003.

[50] Computer Manufacturing Enterprise Security. Threat Agent Library Helps Identify Information Security Risks. Technical report, Intel Corporation, 2007.

[51] Norsk Tipping. Lotto. https://www.norsk-tipping.no/selskapet/produkter/lotto.

[52] Norsk Tipping. Lotto-historikk. https://www.norsk-tipping.no/lotto/om-lotto/lotto-historikk.

[53] Norsk Tipping. Vinnersannsynlighet. https://www.norsk-tipping.no/produktinfo/vinnersannsynlighet.

[54] Wikipedia. Risk. http://en.wikipedia.org/wiki/Risk.

[55] Robert L. Winkler. Uncertainty in Probabilistic Risk Assessment. *Reliablility Engineering and System Safety*, 54(2-3):127–132, 1996.

Del IV

Appendix

TILLEGG A

Intervjuspørsmål

Jeg benyttet meg av et semistrukturert intervju da jeg intervjuet mnemonics konsulenter, og her er spørsmålene jeg gikk ut ifra.

- Hvorfor utførte du RoS-analysen?
  - Uttalt og uuttalt formål? (var det avvik mellom disse?)
- Hva bestod dokumentanalysen av?
- Hvem valgte deltagere til workshop og intervju?
  - Hvorfor ble disse valgt?
  - Hvordan ble disse gjennomført?
- Hvordan var det generelle kunnskapsnivået i gruppene?
  - Både hva angår organisasjonens sikkerhetspolicy og sikkerhet generelt?
- Var det utviklet en fullstendig sikkerhetspolicy hos kunden før analysen?

  - Hvis ja; var denne “god”?
  - Hvis nei; merket man behov for dette underveis?

- Ble det benyttet rammeverk for å definere trusselagentene?
- Ble det tatt ibruk scenarier for å definere risiko?
  - Var scenariene forhåndsdefinerte (eks. SANS)?
  - Hvis ja, hvilke scenarier ble benyttet? Hvis nei, hvem definerte scenariene? Konsulent? Bruker? Oppdragsgiver? Gruppe?
  - Hvorfor ble akkurat disse scenariene benyttet?
- Hva slags metrikker ble benyttet?
  - Hvordan ble nivåene (L/M/H/1/.../n) slått fast?
  - Hvorfor ble akkurat disse metrikkene benyttet?(L/M/H/1/.../n)
- Hadde organisasjonen satt seg et akseptansenivå før analysen?
  - Ble dette nivået endret underveis?
- Hvor dedikerte opplevde du at de ansatte var?
  - Hvor dedikerte var ledergruppen?
- Hvilken grad av modenhet synes du organisasjonen hadde før RoS-analysen?
- Hvilken grad av modenhet hadde de etter analysen?
- Lærte organisasjonen noe?
  - Fikk de noe annet enn analysen ut av oppdraget?
- Hva var de største utfordringene i oppdraget, og hvorfor?
- Hva ville du gjort annerledes?

- Hvor viktig mener du ISO 27005 var for at oppdraget skulle lykkes?
  - I hvilken grad benyttet du standarden?
  - Var vedleggene nyttigere enn selve standarden?
  - Måtte du støtte deg på andre rammeverk?
  - Ønsket du å støtte deg på andre rammeverk?
- Var risikoanalysen en suksess; fikk kunden noe matnyttig ut av oppdraget?

I tillegg til disse spesifikke spørsmålene ble det også spurt logiske oppfølgerspørsmål der jeg følte at det var mer informasjon som kunne avdekkes.

f

TILLEGG B

Ordliste

Her kommer det en ordliste over ordene jeg har benyttet, og hva jeg har lagt i dem.

- **Due Diligence** - Forholdsregler det er rimelig å forvente at en organisasjon/bransje tar for å beskytte seg
- **Due care** - at man utviser aktsomhet
- **Føre var** - Forholdsregler som går godt ut over **due diligence**
- **(Security) control** - virkemiddel
- **Security** - visshet/trygghet
- **Awareness** - bevissthet
- **Arbitrær** - ugjennomtenkt/lite kvalifisert estimering av verdi
- **Risikovurdering** - en helhetlig vurdering av risikosituasjonen
- **Risikoanalyse** - kun en gjennomgang av konsekvens/sannsynlighet

- **Risikoestimering** - raskt overslag over antatt risiko
- **Business Impact Analysis** - konsekvensanalyse
- **Threat Intelligence** - trusseletterretning
- **Scope** - omfang/virkeområde
- **Compliance** - Etterlevelse/være i samsvar med